bB

WRIT (FOR THE MAIN ACTION)

Today,.....two thousand and twenty,

at the request of

1. The foundation **The Privacy Collective**, with registered office in Amsterdam and personal place of business at 3511 GM Utrecht at Catharijnesingel 73;

   choosing as its address for service in this matter the offices of Brandeis B.V. located at Sophialaan 8, 1075 BR Amsterdam, from which offices *mr* [= LLM] Chr. A. Alberdingk Thijm and *mr* F.M. Peters have been appointed by the plaintiff as lawyers and who will act in this capacity with the right of substitution;

SUMMONS THE FOLLOWING, NAMELY:

1. The private limited company **Oracle Nederland B.V.**, with registered office in Utrecht and principal place of business at Hertogswetering 163, 3543 AS Utrecht, serving my bailiff's notification at that address and leaving a copy of it with:

2. The private limited company **SFDC Netherlands B.V.**, with registered office in Amsterdam and principal place of business at Gustav Mahlerlaan 2970 in 1081 LA The Edge, Amsterdam, serving my bailiff's notification at that address and leaving a copy of it with:

3. the company under foreign law **Oracle Corporation**, with registered office in Redwood Shore and principal place of business at 500 Oracle Parkway, Redwood Shores, CA 94065 California, United States, which has no known place of business in or known actual residence in the Netherlands.

   Consequently, by virtue of Article 55 paragraph 1 of the Rv (Dutch Code of Civil Procedure) I have served my bailiff's notification to the official of the Public Prosecutor's office at the Amsterdam District Court, where I left two copies of this writ at the address IJdok 163, 1013

MM Amsterdam, whose translation in the English language will be sent subsequently without delay, which I left with:

who is employed there and was present.

It is requested that this bailiff's notification, provided with a translation of these documents in the English language, be served on **Oracle Corporation** or that the latter be given notice of it, in accordance with Articles 3 to 6 inclusive of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters dated 15 November 1965 (the 'Convention') and this through the serving or giving notice of it with due observance of the procedural rules in the legislation of the member state prescribed for the serving or giving notice about documents that have been drawn up in that country and are intended for persons located there, with the (central or other) authority referred to in Article 6 of the Convention also being asked to return a copy of this bailiff's notification, accompanied by the declaration as referred to in Article 6 of the Convention.

Furthermore that a copy of this bailiff's notification provided with a translation of these documents in the English language was sent by me without delay by registered letter and by UPS courier to the address of the aforementioned **Oracle Corporation** and furthermore that I, in accordance with Article 10 under b of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters dated 15 November 1965 (the 'Convention'), today sent a copy of this bailiff's notification without exhibits, with a translation of it in the English language, to a bailiff, official or other person competent to this end in the state of California (United States of America), with the request to serve it or give notice of it to **Oracle Corporation,** with due observance of the procedural rules prescribed in the legislation of the state of California (United States of America).

4. The company under foreign law **Oracle America, Inc.**, with registered office in Redwood Shores and principal place of business at 500 Oracle Parkway, Redwood Shores, CA 94065 California, United States, which has no known place of business or known actual residence in the Netherlands.

Consequently, by virtue of Article 55 paragraph 1 of the Rv (Dutch Code of Civil Procedure) I have served my bailiff's notification to the official of the Public Prosecutor's office at the Amsterdam District Court, where I left two copies of this writ at IJdok 163, 1013 MM Amsterdam, whose translation in the English language will be sent subsequently without delay, which I left with:

who is employed there and was present.

It is requested that this bailiff's notification, provided with a translation of these documents in the English language, be served on **Oracle America, Inc.** or that the latter be given notice of it, in accordance with Articles 3 to 6 inclusive of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters dated 15 November 1965 (the 'Convention') and this through the serving or giving notice of it with due observance of the procedural rules in the legislation of the member state prescribed for the serving or giving notice about documents that have been drawn up in that country and are intended for persons located there, with the (central or other) authority referred to in Article 6 of the Convention also being asked to return a copy of this bailiff's notification, accompanied by the declaration as referred to in Article 6 of the Convention.

Furthermore that a copy of this writ, provided with a translation of these documents in the English language, was sent by me without delay by registered letter and by UPS courier to the address of the aforementioned **Oracle America, Inc.** and furthermore that I, in accordance with Article 10 under b of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters dated 15 November 1965 (the 'Convention'), today sent a copy of this bailiff's notification without exhibits, with a translation of it in the English language, to a bailiff, official or other person competent to this end in the state of California (United States of America), with the request to serve it on or give notice of it to **Oracle America, Inc.,** with due observance of the procedural rules prescribed in the legislation of the state of California (United States of America).

5. The company under foreign law **Salesforce.com, Inc,** with registered office in San Francisco and principal place of business at 415 Mission St, 3rd Floor, Salesforce Tower, San Francisco, California, CA 94105, United States of America, which has no known place of business in or known actual residence in the Netherlands;

Consequently, by virtue of Article 55 paragraph 1 of the Rv (Dutch Code of Civil Procedure) I have served my bailiff's notification to the official of the Public Prosecutor's office at the Amsterdam District Court, where I left two copies of this writ at IJdok 163, 1013 MM Amsterdam, whose translation in the English language will be sent subsequently without delay, which I left with:

who is employed there and was present.

It is requested that this bailiff's notification, provided with a translation of these documents in the English language, be served on **Salesforce.com, Inc.** or that the latter be given notice of it, in accordance with Articles 3 to 6 inclusive of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters dated 15 November 1965 (the 'Convention') and this through the serving or giving notice of it with due observance of the procedural rules prescribed in the legislation of the member state for the serving or giving notice about documents that have been drawn up in that country and are intended for persons located there, with the (central or other) authority referred to in Article 6 of the Convention also being asked to return a copy of this bailiff's notification, accompanied by the declaration as referred to in Article 6 of the Convention.

Furthermore that a copy of this writ, provided with a translation of these documents in the English language, was sent by me without delay by registered letter and by UPS courier to the address of the aforementioned **Salesforce.com, Inc.** and furthermore that I, in accordance with Article 10 under b of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters dated 15 November 1965 (the 'Convention'), today sent a copy of this bailiff's notification without exhibits, with a translation of it in the English language, to a bailiff, official or other person competent to this end in the city of San Francisco (United States of America), with the request to serve it or give notice of it to **Salesforce.com, Inc.,** with due observance of the procedural rules prescribed in the city of San Francisco (United States of America).

TO:

Appear on **Wednesday 9th December two thousand and twenty (9.12.2020) at 10.00 A.M. CET**, – not in person but represented by a lawyer – at the court session of the Amsterdam District Court, civil-law team, commercial division, to be held in one of the offices of the court building in Amsterdam located at Parnassusweg 220 in (1076 AV) Amsterdam, the Netherlands;

WITH NOTICE THAT:

a. if a defendant fails to appoint a lawyer or fails to pay the court fee stated below promptly and the prescribed deadlines and formalities have been complied with then the district court will declare this defendant to be in default of appearance and will grant the claims described below, unless this appears to the court to be wrongful or groundless;

b. if at least one of the defendants appears in the proceedings and has paid the court fee promptly then a single ruling will be pronounced between all the parties that will be considered to be a ruling in a defended action;

c. if all defendants appear in the proceedings then a court fee will be levied that is to be paid within four weeks calculated from the date of appearance.

d. the amount of the court fees is set out in the most recent annex to the Dutch Court Fees (Civil Cases) Act that can be found for instance on the website www.kbvg.nl/griffierechtentabel;

e. if a person is of limited means then a court fee for people of limited means that is set by or by virtue of the law will be levied, if he (or she) has by the date that the court fee is levied handed over the following:
   - 1st, a copy of the decision granting legal aid that is referred to in Article 29 Dutch Legal Aid Act or, if this is not possible due to circumstances that cannot be reasonably attributed to him, a copy of the application referred to in Article 24 second paragraph Dutch Legal Aid Act, or
   - 2nd, a declaration by the management board of the Dutch Legal Aid Board as referred to in Article 7 under e of this Act that shows that his income does not exceed the incomes referred to in the order in council by virtue of Article 35 second paragraph of that Act;

f. only a single joint court fee will be levied on defendants who appear with the same lawyer and who make identical statements of defence or pursue an identical defence, this on the basis of Article 15 of the Dutch Court Fees (Civil Cases) Act;

g. the exhibits that are part of this writ will be sent subsequently without delay.

WITH NOTIFICATION THAT:

no later than two days after filing the writ, the Plaintiff will file the writ summons with the court registry and will at the same time record the writ in the Central register for collective legal actions as referred to in Article 305a seventh paragraph of Book 3 of the BW (Dutch Civil Code), see www.rechtspraak.nl/Registers/centraal-register-voor-collectieve-vorderingen. The entry will be accompanied by a copy of the writ.

bB

INDEX

TERMS, DEFINITIONS AND ABBREVIATIONS

Technical terms

Term	Definition
Ad tech or **Advertising technology**	Collective name for companies who are active in providing advertisements via the Internet
Advertising space	Part of a webpage that is reserved for the displaying of advertisements
Advertiser or **Marketer**	Advertiser, the party who purchases the advertising space
Publisher	Holder of a website and seller of advertising space
Ad exchange	Auction house where advertising space is traded
Bid request	Request by a Publisher to bid for advertising space. The bid request is sent - together with the Internet user's personal data – to one or more Ad exchanges, who pass on the request to Advertisers
DSP or **Demand Side Platform**	Specialised in purchasing the most suitable advertising space on behalf of Advertisers
SSP or **Supply Side Platform**	Specialised in selling advertising space on behalf of a Publisher
RTB or **Real Time Bidding**	The process in which advertising space is traded via Ad exchanges. Publishers (via SSPs) offer advertising space on their websites for sale, with Advertisers (via DSPs) bidding to display advertisements in this advertising space
DMP or **Data Management Platform**	Specialised in the collecting, managing and enriching of data about Internet users, in the placing of cookies and the exchanging of data by means of cookie syncing, and in the creating of profiles to display the most appropriate advertisements to the Internet user in question
CTR or **Click-through Rate**	Percentage of the total number of displayed advertisements on which a user clicks
Cookie	Small text file that is placed on the website visitor's computer when visiting the website, in which information can be stored
First-party cookie	Cookie that is placed by the website that the user is visiting. For instance, if a user is visiting website nieuws.nl then a cookie placed on the user's computer by nieuws.nl is a first-party cookie
Third-party cookie	Cookie that is placed by the website that the user is visiting. For instance, if a user is visiting website nieuws.nl then a cookie placed on the user's computer by a domain other than nieuws.nl is a third-party cookie
Cookie ID	Unique identifier, stored in a cookie, with which the visitor can be recognised each time he re-visits that same website
Cookie syncing	The exchanging of Cookie IDs between various parties in the ad tech market, so that all these parties find it easy to communicate with each other about a person
First-party data	A Publisher's or Advertiser's own data
Second-party data	Name given by Oracle to data that originates from a service other than Oracle itself. For example, data that is collected by Oracle's AddThis service
Third-party data	Data from parties other than the DMP or the Publisher itself, including data procured from data partners and from other data traders
Profiling	Evaluating the personal characteristics of consumers, with the aim of analysing or predicting consumers' personal preferences, interests,

	behaviour and other characteristics. Profiling is often done using a combination of First-party and Third-party data
DNT or **Do Not Track**	Browser setting with which users automatically send a request to third parties to not be tracked. The request is not stipulated from a technical point of view.
Partner Cookie Policy	A cookie policy is a website's information page about the cookies placed via the website. In the case of a DMP, this is known as a Partner Cookie Policy.
Landing page	'Front page' (homepage) of a website

Abbreviations

Abbreviation	Definition
ACM	the Netherlands Authority for Consumers and Markets (Autoriteit Consument & Markt)
Division	Administrative Jurisdiction Division of the Dutch Council of State
Dutch DPA (in Dutch, the 'AP')	the Dutch Data Protection Authority ('Autoriteit Persoonsgegevens')
GDPR (in Dutch, the 'AVG'	the General Data Protection Regulation (the 'Algemene Verordening Gegevensbescherming')
DMP	Data Management Platform
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ECHR	European Court of Human Rights
EEA	European Economic Area
EU	European Union
ECHR	European Convention on Human Rights
FTC	Federal Trade Commission (USA)
Charter	Charter of Fundamental Rights of the European Union (CFREU)
CJEU	Court of Justice of the European Union
ICO	Information Commissioner's Office (UK)
NDP/Narrowly Defined Group	Disadvantaged persons whose interests are being stood up for in these legal proceedings
Privacy Shield Decree	EU-US Privacy Shield Framework Decree
Tw	Dutch Telecommunications Act
GDPR (I)	GDPR Implementation Act
TOEU	Treaty on the European Union
TOFEU	Treaty on the Functioning of the European Union (in Dutch: 'VWEU')
WAMCA	Dutch Act on the Resolution of Mass Claims in Collective Action ('Wet afwikkeling massaschade in collectieve actie')
Wbp	The Dutch Personal Data Protection Act [now replaced by the GDPR] ('Wet bescherming persoonsgegevens')
WG29	Article 29 working group (succeeded by the EDPB)

1 INTRODUCTION

1.1 Heart of the legal action

1. This legal action relates to one of the largest unlawful data processings in the history of the Internet. It relates to the processing of personal data of practically all Dutch people[1] who read - or view - information on the Internet. It relates to a processing that is not limited in its duration and that is taking place every day on a large scale. The processing solely takes place for commercial purposes, without justification. It has led to (data on) the personal characteristics of everybody who is online being continually unlawfully collected and exchanged, without Internet users knowing about this.

2. Oracle and Salesforce collect - as part of a service that is also known as the Data Management Platform ('**DMP**') - on an unprecedented scale personal data of and about Internet users, which they process into detailed profiles and sell this information to third parties so that the latter can (amongst other things) offer personalised advertisements on websites. The data collection process starts with Oracle and Salesforce placing a cookie[2] on the terminal equipment of the Internet user. This cookie is equipped with a unique identifier that is used to distinguish between different Internet users. The cookie is used to collect personal data such as the Internet user's IP address. Oracle and Salesforce track the Internet user across different devices that he (or she) uses and in doing so also collect other unique identifiers such as those of a mobile telephone or pseudonymised e-mail addresses. In this way, a 'fingerprint' of the user is created to which a unique profile is attached.

3. Oracle and Salesforce enrich the information gathered via the cookie and other unique identifiers with information from alternative sources. This relates not only to online buying (and clicking) behaviour but also to information from offline sources, such as from a supermarket's loyalty programme. In this way, Oracle and Salesforce add to the profile every day and build it up, so that as complete a picture as possible is created of the character traits and interests of the person in question. Oracle and Salesforce provide advertisers with the means to segment Internet users and to create a unique 'audience'.

4. The purpose of these data processings includes the sharing of the profile of the Internet user as part of a process that is known as Real Time Bidding ('**RTB**'). Any person who visits a website becomes the subject of an auction process without realising it. In a fraction of a second, even before the website has loaded, the profile of the Internet user, including his preferences and interests, are offered to as many as hundreds of parties. The parties use the information to bid for the space so that they can display an advertisement to the Internet user. The highest bidder wins, which means he can then display an advertisement that is the best possible match with the characteristic traits and interests of the Internet user. During this process, unique

[1] In this writ, for the sake of clarity we talk about 'Dutch people' and 'Dutch Internet users' but what is meant is all those persons who have used the Internet within or from the Netherlands since the GDPR (the General Data Protection Regulation) became applicable.
[2] A cookie is a text file that a website holder or third party can place on the Internet user's device when the latter visits a website or performs another online action, this placing being done to collect information that is used later on. Cookies can have a useful application for the Internet user, for instance to store passwords so that the Internet user does not have to enter them anew each time he visits the website but they can also be used for instance to collect data to create a profile of an Internet user.

identifiers are then exchanged with other commercial parties and linked up with each other. This process is known as 'cookie syncing', more of which later in this writ.

5. All this is done automatically and without the Internet user being aware of it.

6. With their DMP service, Oracle and Salesforce play a crucial role in the RTB process. In this process, Oracle and Salesforce place the cookies on the terminal equipment and other devices of the Internet user. Oracle and Salesforce enrich the data and are responsible for the exchanging of the unique identifiers and the information linked to them, so that as complete a picture as possible of the Internet use (and user) is built up. In this way, the enriched profile becomes an item in the auction process.

7. In this legal action, the Foundation The Privacy Collective (hereinafter also known as the 'Foundation') intends to call a halt to this way of doing business and to obtain compensation for the harm suffered by the persons whose interests it is representing.

1.2 Summary

8. In this writ, first of all the importance of this legal action will be outlined (see marginal note **1.3**), including references to the large number of complaints submitted by regulatory authorities, which have not however - so far - led to the imposing of any sanctions against Oracle and Salesforce or other parties. The Foundation is of this opinion that this legal action is the sole remaining option for effective enforcement, namely for demanding compensation in a class action that does justice to the violations of both the right to privacy and the right to data protection that are systematically occurring in the case in question.

9. The position of and role played by the Foundation will then be explained (section **2**). Next, the technical procedures deployed by Oracle and Salesforce will be looked at (section **3**). This requires a description of the RTB process and of the parties that are active in this market. It is technically complex material. This section will also look at the way in which the Foundation has had research carried out by a technical expert into the procedures deployed by Oracle and Salesforce.

10. Following this, the legal framework will be looked at (section **4**). This section will look in detail at how Oracle and Salesforce violate fundamental rights every day and infringe a large number of provisions from the General Data Protection Regulation (the '**GDPR**')[3] and the Dutch Telecommunications Act (the '**Tw**'). To this end, first of all the relevant fundamental rights will be discussed, including in the light of the great importance that the Court of Justice of the European Union (the '**CJEU**') attaches in its court rulings to strict compliance with the fundamental rights from the Charter of Fundamental Rights of the European Union (the '**Charter**').

11. It will be shown that Oracle and Salesforce process personal data on an enormous scale within the meaning of the GDPR and are the (joint) controllers for this processing. The territorial applicability will be substantiated too.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation) ('GDPR')

12. This will be followed by a discussion of the principles and provisions of the GDPR and the Tw that Oracle and Salesforce are infringing. The Foundation will demonstrate that Oracle and Salesforce are systematically infringing the GDPR, including by:

    i. drawing up and maintaining detailed profiles of Internet users ('profiling') and using these for automated processings that significantly affect these users ('automated decision-making');

    ii. collecting and processing the data of Internet users without a lawful basis for doing so, for example by placing cookies on Internet users' terminal equipment and other devices without valid consent;

    iii. failing to be transparent enough about their conduct, for example in respect of the exchanging of unique identifiers from cookies with other parties ('cookie syncing');

    iv. acting contrary to the requirement of data minimisation, by collecting, combining and sharing personal data unrestrictedly and excessively;

    v. processing personal data contrary to the purposes for which it was originally collected, by failing to have sufficient suitable data security measures in place, by acting contrary to their duty of responsibility and by passing on personal data to countries that have no appropriate data protection regime.

13. Oracle and Salesforce will be discussed, as will their duty to compensate these Internet users for the harm they are suffering and have suffered (section **5**). The primary basis for compensating the harm suffered is the violation of the relevant fundamental rights and the infringement of the GDPR and the Tw. Also given the nature, the seriousness, the duration and the deliberate nature of these violations, this harm for each party is estimated to be € 500 per person per defendant (to which figure is to be added with regard to Oracle the sum of € 100 per person due to a data breach that is still to be discussed);

14. The Foundation invokes both alternatively and, as a second alternative, the liability of Oracle and Salesforce by virtue of the unlawful act and unjustified enrichment. In so far as additional controllers or data processors are involved in the activities of Oracle and Salesforce, it will be explained why they have joint and several liability for the harm that the processing causes. Next, the claim for relief will be explained (section **6**), along with a discussion of the aspects of the case that relate to the law of evidence (section **7**), a section about the Foundation's independence (section **8**), an explanation of the jurisdiction and applicable law (section **9**) and a refutation of the defences put forward by Oracle and Salesforce (section **10**).

1.3 Importance of this case

15. The system that Oracle and Salesforce maintain and facilitate is being attacked from all sides internationally, including by both politicians and society. For example, the unbridled data processing carried out for RTB has been severely criticised in both the US and the European Union. Regulatory authorities all over the world are being called on to halt these practices.

16. In the USA, on 31 July 2020 senators and members of Congress of both the Republican Party and the Democratic Party sent a letter to the American regulatory authority that is the Federal

Trade Commission (the '**FTC**'), asking it to intervene and halt the unparalleled privacy violations that are being carried out every day via RTB[4]. 'This outrageous privacy violation must be stopped and the companies that are trafficking in Americans' illicitly obtained private data should be shut down,' they wrote in a letter to the FTC that is signed by ten senators and members of Congress, including Elizabeth Warren. In the letter, they refer to investigations being carried out by regulatory authorities in the European Union.

17. Privacy and human rights organisations have submitted complaints to at least 14 European regulatory authorities in respect of the protection of privacy and personal data. This has happened in Poland[5], Belgium, Spain, Luxembourg[6], Germany, France, Italy, Hungary, Bulgaria, the Czech Republic, Estonia, Slovenia[7], the Netherlands and Ireland.[8] In May 2019 in the Netherlands, the foundation Bits of Freedom submitted a complaint to the Dutch Data Protection Authority (the 'AP') regarding infringements of the rights of Dutch persons in the RTB market[9].

18. On 8 November 2018, Privacy International submitted complaints to the British regulatory authority the Information Commissioner's Office (the '**ICO**') about the processing of personal data by data traders. The complaint was aimed at Oracle (as well as at other parties) because Oracle - through aggregation and tracking - divides data subjects into thousands of categories. Analysis of the British market reveals that Oracle possesses 180.7 million unique IDs and divides data subjects into 58,800 different interest segments.[10] The complaints also relate to six other data traders and have been filed in France, Ireland and the United Kingdom.[11]

19. On 6 April 2020, the Irish regulatory authority for privacy[12] published a report about the tracking technologies.[13] The regulatory authority looked in particular at the way in which information is provided to and consent obtained from Internet users that visit websites. The regulatory authority's conclusions included that of the 38 websites investigated, only two substantially complied with the GDPR.

20. According to this regulatory authority, not even the most basic information is provided about Internet users giving their lawful consent to the placing of cookies. Internet users have no idea about the extent to their devices at home and at work are being tracked:

> *'Lacking even basic information or the ability to give unambiguous consent for the placement of tracking technologies or cookies on their devices, most ordinary users*

[4] Letter from senators and members of the US Congress to the FTC dated 31 July 2020, which may be obtained for instance from: https://www.adexchanger.com/privacy/lawmakers-call-rtb-an-unfair-and-deceptive-business-practice-in-letter-to-the-ftc/
[5] https://techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/.
[6] https://techcrunch.com/2019/05/20/gdpr-adtech-complaints-keep-stacking-up-in-europe/.
[7] https://www.tijd.be/tech-media/media-marketing/privacyklachten-tegen-hoe-google-advertenties-verdeelt/10140271.html.
[8] https://www.dataprotection.ie/and/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and.
[9] https://www.bitsoffreedom.nl/wp-content/uploads/2019/05/20190520-handhavingsverzoek-iab-google-openbaar.pdf.
[10] https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf, p. 6.
[11] https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.
[12] The Data Protection Commission or DPC.
[13] https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf.

will not be aware of the extent to which they may be tracked across their devices at home and at work, and across their browsing, reading and social habits.'[14]

'The fact that bad practices were widespread even among companies and controllers that are household names suggests a more systemic issue that must be tackled firstly with the publication of new guidance, followed by possible enforcement action where controllers fail to voluntarily bring themselves into compliance.'[15]

21. An investigation by the Irish regulatory authority on privacy into the ad tech industry and RTB is still ongoing.[16]

22. The British agency ICO is very critical too. On 20 June 2019, the ICO published a report about the *ad tech* and RTB market (**Exhibit 1**).[17] The conclusions reached by this regulatory authority included the fact that the ad tech market is ignoring the right to data protection. The ICO states that insufficient data is provided to the data subjects. This regulatory authority also concluded that very detailed profiles are created and exchanged between hundreds of parties, all this without the data subjects being aware of this.

'profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individual's knowledge.'[18]

23. In January 2020, the Norwegian consumer association published its detailed report, including technical analysis, into the use of personal data in much-used apps.[19] This Norwegian consumer association noted that the tracking and profiling of Internet users takes place on an ongoing basis:

'As we move around on the internet and in the real world, we are being continually tracked and profiled for the purpose of showing targeted advertising. In this report, we demonstrate how every time we use our phones, a large number of shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour.'[20]

24. This Norwegian consumer association describes the role played by DMPs in the *ad tech* market as the service that makes it possible for website holders and advertisers to combine their own data with that from third parties. DMPs are described as data traders that manage gigantic identity databases that are used to link up profiles between various parties:

'Data management platforms are used by publishers and marketers to combine data on their existing customers, including behavioural data collected from their websites and apps, with data from third party providers. They provide mechanisms to further analyse and refine data on consumers, and then analyse

[14] Page 18.
[15] Report by the [Irish] Data Protection Commission on the use of cookies and other tracking technologies, pp. 18 and 19.
[16] https://www.dataprotection.ie/and/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and.
[17] Information Commissioner's Office, *Update report into AdTech and real time bidding*, 20 June 2019 (**Exhibit 1**), can be consulted via: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[18] Page 23.
[19] https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/.
[20] Out of control, page 5.

and utilize it across the web, mobile apps and other services. As a part of the RTB process, DMPs also provide instructions to DSPs about which consumers to target based on the profiles that they compile.

As data management platforms often resell large amounts of third-party data to many clients, in addition to compiling and combining the data, they can also be categorized as a type of data broker. Most of them maintain massive identity databases that help other companies to link digital profiles across contexts and vendors.'[21]

25. This Norwegian consumer association also states that Oracle and Salesforce (and other companies) are part of the group of the 'major DMP vendors':

'Major DMP vendors include Oracle, Adobe, Salesforce, Nielsen, Neustar, Lotame, The ADEX, KBM Group (owned by the major advertising agency group WPP). Several AdTech companies also provide DMP functionality, including MediaMath, AdForm, and Google.'[22]

26. In the Netherlands, this report led to a campaign by the Dutch Consumers' Association under the name 'Data sharers: illegal data trading'[23] and to Parliamentary questions being put to the Dutch Minister for Legal Protection Sander Dekker.[24]

27. In June 2020, the European Commission's evaluation of the GDPR concluded for instance that strict enforcement against companies in the advertising sector was necessary to protect individuals, especially in the field of online advertising and 'behavioural targeting':

'In addition, vigorous enforcement of the GDPR in respect of major digital platforms and integrated companies, including in such areas as online advertising and microtargeting, is essential to be able to protect people.' 25

28. Despite the above, on 7 May 2020 the British regulatory authority ICO announced that it was temporarily suspending its investigation into RTB and the ad tech industry. The ICO has stated that during the Covid-19 crisis it did not wish to place any 'undue pressure' on the industry, despite its concerns about ad tech. It also appears that a halt has been called to the Dutch Data Protection Authority's investigation that followed on from the claims made by the Bits of Freedom.

29. Interest groups have stated that the real reason that their complaints are not being followed up on is that the regulatory authorities are suffering from a lack of resources, including a

[21] Out of control, p. 37.
[22] Out of control, p. 37, footnote 89.
[23] https://www.consumentenbond.nl/acties/datadealers, consulted on 30 April 2020.
[24] https://www.tweedekamer.nl/downloads/document?id=8e05af88-94d8-4f86-9998-68aecebd4779&title=Het%20bericht%20dat%20de%20Consumentenbond%20de%20noodklok%20luidt%20om%20illegale%20datahandel%20.pdf, consulted on 30 April 2020.
[25] European Commission, Statement from the Commission to the European Parliament and the Council, 'Data protection as a cornerstone of the power enjoyed by citizens and the EU approach to digital transformation — two years of applying the GDPR', 24 June 2020 (COM(2020) 264 final), can be consulted via: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52020DC0264.

chronic lack of personnel.[26] It is a complex market in which a multiplicity of players operate, largely behind the scenes.

30. It is in this playing field that the Foundation asks Your Court to hold Oracle and Salesforce responsible for the way in which - every day - they are violating the fundamental rights of Internet users and infringing both the GDPR and the Tw. The Foundation asks Your Court to do this in a way that does justice to the harm that Internet users are suffering every day as a result of their actions and to also do so in a way that is sufficiently effective and deterring.

31. Time after time, the CJEU has confirmed the importance of being highly protective of the right to the protection of privacy and the right to data protection. It follows from CJEU court rulings that a situation must be prevented where the relevant parties fail to take responsibility. It must be ensured that data subjects are guaranteed that their rights will be protected effectively and completely.[27]

32. It is striking that many of the interesting court rulings of the CJEU have been initiated by interest groups or privacy activists. In the *Breyer* case, the CJEU confirmed the broad scope of the term 'personal data' and that this term had to include IP addresses.[28] This legal action was instituted by Patrick Breyer, Euro MP and activist in the field of digital rights, against the German State. The Austrian Max Schrems, lawyer and privacy activist, is now known all over the world for twice getting the exchange of data between (parties in) the European Union and the US stopped.[29] The interest group Digital Rights Ireland's efforts ensured that the CJEU ruled that the Data Retention Directive - a directive that stipulated that telecom providers had to store location data - was invalid.[30] In the *Fashion ID* case, the German consumer organisation Verbraucherzentrale NRW induced the CJEU to clarify the definition of the term '(data processing) controller'.[31] In the *Planet49* case, the German consumer organisation Verbraucherzentrale Bundesverband's efforts ensured that the CJEU answered questions about interpretation, including about the interpretation of the consent requirement for the placing of cookies.[32]

33. Ensuring a high level of protection and an effective and comprehensive protection of the fundamental rights relating to the protection of privacy and data protection ensures that member states have to take all appropriate measures to ensure full compliance with the GDPR.[33] This is why the GDPR feels that private enforcement is important and so offers much scope for the representation of collective interests. Article 79 GDPR guarantees the right to effective relief in law, this without prejudice to the right to submit a complaint to the regulatory (or supervisory) authority. Article 80 GDPR gives data subjects the right to have themselves represented by a non-profit organisation. This explicitly relates too to the option to exercise the right to compensation by virtue of Article 82 GDPR. The Dutch system set out in Article 3:305a BW (Dutch Civil Code) is especially suitable for this.

---

[26] See https://www.itpro.co.uk/policy-legislation/data-protection/356423/ico-lambasted-for-falling-asleep-at-the-wheel
[27] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13.
[28] CJEU 19 October 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer*).
[29] CJEU 6 October 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*) and CJEU 16 July 2020, C-311/18, ECLI:EU:C:2020:559, (*Schrems II*).
[30] CJEU 8 April 2014, case c-293/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*).
[31] CJEU 29 July 2019, , C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*).
[32] CJEU 1 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[33] See also CJEU 29 July 2019, , C-40/17 (*Fashion ID*), ECLI:EU:C:2018:1039, legal grounds 50 and 59.

34. What makes this legal action unique and sets it apart from the examples quoted above is that, as far as is known, this is the first time that compensation is being claimed under the GDPR as part of a class action.

2 THE PARTIES

2.1 Foundation The Privacy Collective

35. The Foundation was set up on 29 May 2020 to bring to an end to the large-scale, unlawful processings of the personal data of Internet users and the associated violation of their privacy rights and to get redress for the people it represents (**Exhibit 2**).

36. The Foundation has both a (management) board and a Supervisory Board.[34] The members of the board and the Supervisory Board possess the specific expertise needed to properly represent the interests as described in the Foundation's Articles.[35]

37. The Foundation does not have a profit motive, with its objects according to its Articles being – stated briefly – to protect the privacy interests and personal data of Internet users:[36]

> *'The objects of the Foundation are to represent the interests of natural persons who use the Internet by surfing on the Internet and/or by using products and/or services that can store, transfer or process personal data in digital form, as a result of which these Internet users could at any time have (or have already had) their right to the protection of their privacy violated or their right to the protection of their personal data violated, the above in the broadest sense of the term.'*

38. The Foundation endeavours to achieve these objects amongst other ways by mounting campaigns, by carrying out technical and other research (including by mandating others to do this) into the large-scale collection and processing of personal data of Internet users and into the parties that play a role in these activities, such as Oracle and Salesforce, and by carrying out research into partnerships with other organisations. The purpose of all this is to get compensation for all those persons whose rights have been violated by the unlawful, large-scale collection and processing of personal data.

39. The Foundation is acting for and on behalf of all Internet users (hereinafter also referred to as the '**Victims**'). As will be shown below, it must be presumed that <u>all</u> the approx. 10 million Dutch Internet users have been harmed by Oracle and Salesforce. Below, in Section 1.1, details will be provided about the fact that when visiting almost all popular commercial websites in the Netherlands, personal data is collected from Dutch Internet users with the help of cookies and other tracking technologies of Oracle and Salesforce.

40. When it comes to the dispute in question, the group of persons who is represented by the Foundation can be divided into two categories, namely the group disadvantaged by Oracle and the group disadvantaged by Salesforce. Together they form an **NDG** or '**Narrowly Defined**

[34] Section 8 goes into the foundation and the admissibility of the Foundation in more detail. That section provides a detailed description of the members of the board and the Supervisory Board and their expertise.
[35] See Article 3 of the Articles of the Foundation (**Exhibit 2**) for a description of the interests represented by the Foundation.
[36] See Article 3 of the Articles of the Foundation (**Exhibit 2**).

Group', as referred to in the WAMCA Act (the Dutch Act on the Resolution of Mass Claims in Collective Action ('Wet afwikkeling massaschade in collectieve actie')).

41. The Foundation is not alone in this. It is supported in the Netherlands by leading (interest) groups and other organisations active in the field of the preservation and promotion of the right to privacy, such as Bits Of Freedom[37], Privacy First[38], Freedom Internet[39] and the Qiy Foundation[40]. In addition, the Foundation works with persons and organisations in other countries where similar steps may be or are being taken. In the light of the Foundation's objects under its Articles, the Foundation is also taking legal action. These legal proceedings are an example of this.

42. In these legal proceedings, the Foundation is instituting a class action for damages against Oracle and Salesforce. In doing so, the Foundation is conducting legal proceedings on the basis of Article 3:305a BW (Dutch Civil Code). The causes of action relate to the protection of the interests of Dutch Internet users whose right to have their privacy and personal data protected has been and is being harmed by Oracle and Salesforce.

43. By registered letter dated 3 June 2020, the Foundation has held both Oracle (**Exhibit 3**) and Salesforce (**Exhibit 4**) accountable for the harm suffered by those it represents as the result of the violations of the right to the protection of privacy and the right to the protection of personal data. The Foundation invited Oracle and Salesforce to start negotiations with the Foundation about awarding reasonable compensation for the harm suffered by those it is representing.

44. Oracle and Salesforce accepted the invitation offered by the Foundation by means of letters dated 18 June 2020 (**Exhibit 5**) and 17 June 2020 (**Exhibit** 6). On 3 July 2020, a consultative meeting took place between the Foundation and Salesforce. On 7 July 2020, such a meeting was also held between the Foundation and Oracle. The consultations conducted with Oracle and Salesforce have not led to the desired result. Oracle and Salesforce have both stated that they see no need for follow-up consultations.

45. Accordingly, the Foundation feels obliged to institute these 'class action' legal proceedings to claim compensation for and on behalf of the people it is representing.

2.2 Oracle and Salesforce

46. Oracle Corporation, Oracle America, Inc. and Oracle Nederland B.V. (hereinafter '**Oracle**') are part of an internationally active technology group that operates in such areas as business software for data management applications. Over the past decade, Oracle has increasingly focussed on the collecting, enriching and selling of Internet users' personal data.

47. Salesforce.com, Inc. and SFDC Netherlands B.V. (hereinafter '**Salesforce**') are likewise part of an internationally active technology group but one in this case that provides such products

[37] https://www.bitsoffreedom.nl.
[38] https://www.privacyfirst.nl.
[39] https://www.freedom.nl/.
[40] https://www.qiyfoundation.org/nl/.

as business software for customer relationship management. In recent years, Salesforce too has developed into one of the leading traders in personal data.

48. The online advertising market is a hugely lucrative one. In 2019, it generated revenue of more than 300 billion dollars.[41] DMP providers such as Oracle and Salesforce earn a large share of this revenue. In 2019, Salesforce's Marketing & Commerce Cloud, which provides such services as the personalisation of advertisements and websites, earned revenue of almost 1.9 billion dollars.[42] As recently as 2017, this figure was 'just' 947 million dollars. There are many players in this market. The trade in personal data is hugely profitable for all the companies concerned.

49. Oracle and Salesforce are very important players in this market. Both parties have invested huge sums in their market position, including by taking over a large number of parties.

50. In recent years, Oracle has taken over the following companies and services:

- Bluekai (approx. 400 million dollars [annual revenue]), a 'big data' platform that focusses on the personalisation of advertising by using 'big data', with as much 'synced' (i.e. linked) data and as many linked profiles as possible;
- AddThis (approx. 200 million dollars), software that allows websites to place buttons so that articles can be shared via social media. These 'share' buttons are also used to collect data;
- Moat (approx. 850 million dollars), specialises in analysing and influencing the 'attention' of the Internet user, doing so via more than 33 billion attention analyses per day;[43]
- Crosswise (approx. 50 million dollars), specialises in cataloguing the devices (laptops, smartphones, tablets, televisions) that belong to the same person;
- Eloqua (approx. 871 million dollars), specialises in the automation of digital marketing;
- Grapeshot (approx. 325 million dollars), specialises in contextual advertising;
- Datalogix (approx. 1.2 billion dollars), specialises in the collection of offline information of and from consumers for online marketing; and
- Responsys (approx. 1.5 billion dollars), specialises in the sending of personalised e-mails.

51. Oracle's DMP is based on what Bluekai used to be. In other words, it's about big data.[44] Oracle combines its DMP with other services such as AddThis, Datalogix, Eloqua, Responsys and Crosswise. This gives Oracle the option in-house to obtain data from many different sources across a range of devices both online and offline and to personalise marketing efforts across a broad range of channels. According to Oracle, by using its DMP its clients (website holders, marketeers and publishers) are obtaining '*more data to drive deeper insights and better*

[41] Magna, *Magna advertising forecasts – winter 2019 update*, 9 December 2019, can be consulted via: https://magnaglobal.com/magna-advertising-forecasts-winter-2019-update/.
[42] https://s23.q4cdn.com/574569502/files/doc_financials/2019/Salesforce-FY-2019-Annual-Report.pdf, pp. 4 and 44, consulted on 4 May 2020.
[43] https://moat.com/.
[44] An introductory film clip by Bluekai (2:24) can be found at: https://www.youtube.com/watch?v=UBmgkZdWGLw, consulted on 29 July 2020.

personalization'[45], along with a '*truly holistic view of customers*'.[46] **Exhibit 7** contains a selection of pages from Oracle's website in which it explains what its DMP consists of.

52. Salesforce too has used acquisitions to take over an important position in the world of data trading: for instance, in 2013, Salesforce took over ExactTarget for the sum of 2.5 billion dollars, and in 2016 Salesforce acquired the company Krux for 700 million dollars. Krux provides a service that optimises marketing efforts by using personal information, which is similar to what Bluekai does. Krux is now part of the Salesforce DMP and goes by the name of 'Salesforce Audience Studio and Data Studio' or the 'Salesforce Marketing Cloud'.

53. With regard to its DMP, Salesforce stated in 2016 that each month, Krux communicates with 3 billion browsers, supports 200 billion 'data collection events' and processes 5 billion profiles. Salesforce describes its way of working as 'orchestrating'. In this way, it orchestrates 200 billion 'personalized consumer experiences':

> *'Salesforce Marketing Cloud empowers marketers in all industries to leverage meaningful customer and prospect data, build personalized customer journeys at scale and drive business performance. And with Einstein, marketers can predict the best audience, content, channel, and send-time for every customer interaction — and recommend the best offer — all automatically. On a monthly basis, Krux interacts with more than three billion browsers and devices, supports more than 200 billion data collection events, processes more than five billion CRM records, and orchestrates more than 200 billion personalized consumer experiences. Salesforce Marketing Cloud's scalable infrastructure, paired with these new artificial intelligence and cross-device identity management capabilities make it uniquely positioned to empower companies to deliver a consistent brand experience throughout the customer journey.'*

54. Salesforce markets the Audience Studio and Data Studio services as a way of obtaining 'deep insights' into Internet users 'across every touchpoint':

> ***'Meet Audience Studio.***
>
> *Formerly Salesforce DMP, Audience Studio can help you gain deep insights by unifying and capturing your data to strengthen customer relationships across every touchpoint with a powerful data management platform.'*[47]
>
> ***'Meet Data Studio.***
>
> *Get to know Salesforce's #1 solution for audience discovery, data acquisition, and data provisioning — featuring the world's most-trusted premium data ecosystem.'*[48]

55. In principle, Salesforce is active in the same field as Oracle and other DMPs, namely large-scale data trading. **Exhibit 8** contains a selection of pages from the Salesforce website in

[45] https://www.oracle.com/the/data-cloud/products/data-management-platform/, consulted on 14 July 2020.
[46] https://www.oracle.com/nl/data-cloud/products/data-management-platform/cross-device.html, consulted on 14 July 2020.
[47] https://www.salesforce.com/products/marketing-cloud/data-management/, consulted on 28 April 2020.
[48] https://www.salesforce.com/products/marketing-cloud/data-sharing/, consulted on 28 April 2020.

which it explains what its DMP consists of. At Salesforce too, a core aspect of its activities is the linking up of a large number of different data sets, whereby it assigns a unique code to each Internet user, builds up a profile and makes each interaction with an Internet user 'personal'.

> *'**Create a single, consistent customer ID**.*
>
> *Unify customer data across multiple teams, devices, and systems, such as email, online behavior, ecommerce, and CRM data.'*
>
> *'**Build effective customer segmentation**.*
>
> *Easily stitch together first-, second-, and third-party data to create and analyze specialized audience segments.'*
>
> *'**Personalize every interaction**.*
>
> *Advertise to the right segments and personas with content tailored across social platforms, online ads, and beyond.'*[49]

56. We will now look at how a DMP works within the ad tech ecosystem in general and how the DMPs of Oracle and Salesforce work in particular.

3. HOW ORACLE & SALESFORCE GO TO WORK

3.1 What is a DMP?

57. Oracle and Salesforce each offer a Data Management Platform ('**DMP**'). A DMP is a service that focusses on collecting and combining data to present visitors to websites with specific advertisements that target that individual person. The DMP service is used by website holders, advertisers, marketeers and other data traders, as will be explained below.

58. Whereas in the offline world, advertisements are placed on the basis of a presumption of the interests and preferences of the collective readership of a newspaper or magazine, new technologies enable advertisers to determine very precisely the interests and preferences of specific Internet users. In 2012, the New York Times reported about an angry father who went to his local Target store (part of a US department store chain) to demand an explanation as to why his 'non-pregnant' teenage daughter was being sent discount vouchers for baby clothes. He also accused Target of encouraging her to get pregnant. Well, it turned out that his daughter WAS actually pregnant but that he, the father, had not been told this. Target had established this fact based on her online shopping behaviour.[50]

59. Since then, the options for finding out precisely who is visiting a particular website have exploded. Thanks to the developments in the field of big data and AI (artificial intelligence), the advertiser often knows more about the website visitor than the latter does himself. In the aforementioned letter from 31 July 2020 that was sent to the FTC, the senators and members

[49] https://www.salesforce.com/products/marketing-cloud/customer-data-platform/, consulted on 6 May 2020.
[50] New York Times, *How companies learn your secrets*, 16 February 2012, consulted via https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp

of Congress state how big data – including location data from mobile phones - was recently used to analyse the participants in a Black Lives Matter protest.[51]

60. Such personalised advertisements are founded on the collection of data about the website visitor in question. This includes demographic characteristics (age, gender etc.), visited websites, apps used, location data, Internet searches, interests and preferences. The reason for this data collection and processing is to induce Internet users to perform a certain action, for example to purchase a product.

3.2 Activities performed by Oracle and Salesforce

61. Oracle and Salesforce play an essential role in these data collection and data processing processes. Oracle describes the DMP as the 'enabler of the digital marketing ecosystem'.

> *'**A DMP Functions as an Enabler of the Digital Marketing Ecosystem***
>
> *Oracle's complete mapping of IDs for consumers, along with mapping to downstream media and app partners, positively influences the addressability and deliverability of marketing campaigns across all digital and mobile, and the overall success rate for marketers to use the data. Thanks to the media integrations the Oracle DMP 'just works' on day one. The integrations are already in place so clients can leverage the scale of our networks on day one.'*[52]

62. The *Cambridge Dictionary* defines an 'enabler' as a person who makes it possible for something to happen or take place. In Dutch, such a person would be called an 'arrangeur' ('arranger'). In other words, the DMP is the party that arranges matters in the online advertising ecosystem in such a way that 'behavioural targeting' can take place.

63. As DMPs, Oracle and Salesforce carry out the following activities, amongst others:

1. the placing of cookies that are equipped with a unique identifier on the Internet user's terminal equipment or other device;
2. using these cookies and other unique identifiers to collect personal information about the Internet user;
3. evaluating personal characteristics of Internet users to analyse and/or predict personal preferences, interests, behaviour and other characteristics. This is known as 'profiling'.
4. the enriching of these profiles and personal data with information from other sources;
5. the creating and providing of profiles, so that third parties can use them to assess in an online auction and how much (if anything) they want to bid for advertising space ('realtime bidding').

[51] See also https://www.wsj.com/articles/lawmakers-urge-ftc-probe-of-mobile-ad-industrys-tracking-of-consumers-11596214541
[52] https://www.oracle.com/nl/data-cloud/products/data-management-platform/ecosystem.html, consulted on 4 August 2020.

6. linking up the cookies' unique identifier with the unique identifiers of the cookies of other AdTech parties, to make data exchange possible ('cookie syncing').

64. They use software to perform these activities automatically. A DMP provides its clients and/or partners with the following resources and services, amongst others:

- a software platform that is being constantly developed and maintained that can be used for the collection, retention and enrichment of data;
- a software system that website holders can use to link up with the Oracle and Salesforce platform to place and read cookies;
- maintaining and providing access to gigantic databases for data storage in which data from various sources are linked up with each other;
- the creating of links between third-party databases and the platform, to enrich data;
- developing and maintaining algorithms, to identify one specific data subject and to track his activities across multiple devices;
- developing and maintaining cookies with unique identifiers and creating technical links between their own cookie identifiers and those of third parties, to identify each other's users and to exchange data;
- developing and maintaining software with which large volumes of data can be structured, organised and made readily comprehensible, using 'big data' techniques
- developing and maintaining algorithms, to create profiles and interest segments from the various data sets;
- providing an interface/dashboard that the clients of Oracle and Salesforce can use to find specific target groups and interest segments.

65. The large volume of data that they collect about Internet users and the (automated and other) analyses that they add to it means that Oracle and Salesforce create an intrusive overview of the online life of individual persons. Internet users are assigned characteristics and are classified into different segments or 'audiences'. Oracle and Salesforce link up various unique identifiers with each other, so that a single 'fingerprint' or 'ID Graph' is created. Oracle and Salesforce are also specialists in the enriching of this data with data from other sources. This may include data about offline purchases, location data, credit card data, financial data and data from social media. Oracle and Salesforce also offer their clients the option of adding their own data. This creates an intrusive picture of somebody's entire life, both his or her online life and their offline life too. This profile is used for such purposes as 'Real Time Bidding ('RTB'), which will now be looked at.

66. With RTB, the advertising space on a website (for example) is sold in 'real time', i.e. at the moment in time when a person visits a website, via an auction. This process proceeds completely automatically, with DMPs playing a crucial role in this regard. Oracle and Salesforce make it possible for advertisers to bid for advertising space based on information.

It is Oracle and Salesforce that collate the information in this context and share it with third parties.

67. Every time that an Internet user visits a website on which advertisements or other personalised content is displayed, an auction is taking place in the background. By using a large set of data that is available about the Internet user, an advertiser can assess whether he wants to bid for the advertising space and if so, for how much. This auction takes place in the time that it takes to load the webpage, i.e. in a fraction of a second.

68. To be able to display a targeted advertisement on a website, personal data about Internet users is collected, combined, enriched and shared. This collecting, combining, enriching and sharing is carried out by means of a DMP.

69. When the advertising space is offered, the data about the visitor is simultaneously shared with hundreds of potential advertisers and marketeers and with the advertisement exchanges (auction houses) they use. The identity of these parties is not known to the other participants in the RTB process or to the visitor. It is not known either what these hundreds of parties do with the data once they have participated in the auction. The DMP makes it possible to serve up advertisements to the right person, which means it plays a crucial role in the RTB process, which is to sell advertising space to the highest bidder on the basis of the Internet user's profile.

70. In this way, Oracle and Salesforce put together completely specific target groups for advertisers. A DMP may do this by analysing the data about the advertiser's own clients and then using this analysis to create an accurate profile of the average client. This profile is then compared with the profiles that a DMP has of website visitors, to display the advertisement to precisely those persons who have this same profile.

3.2.1 The placing of cookies

71. Oracle and Salesforce use cookies and similar techniques to collect the data that is then used to create the profile of the Internet user. For Internet users, cookies can have a useful application too. Cookies are text files that a website holder or third party can place on the user's computer to collect information for subsequent use. Cookies can for example recognise Internet users so that they do not have to enter their passwords again each time.

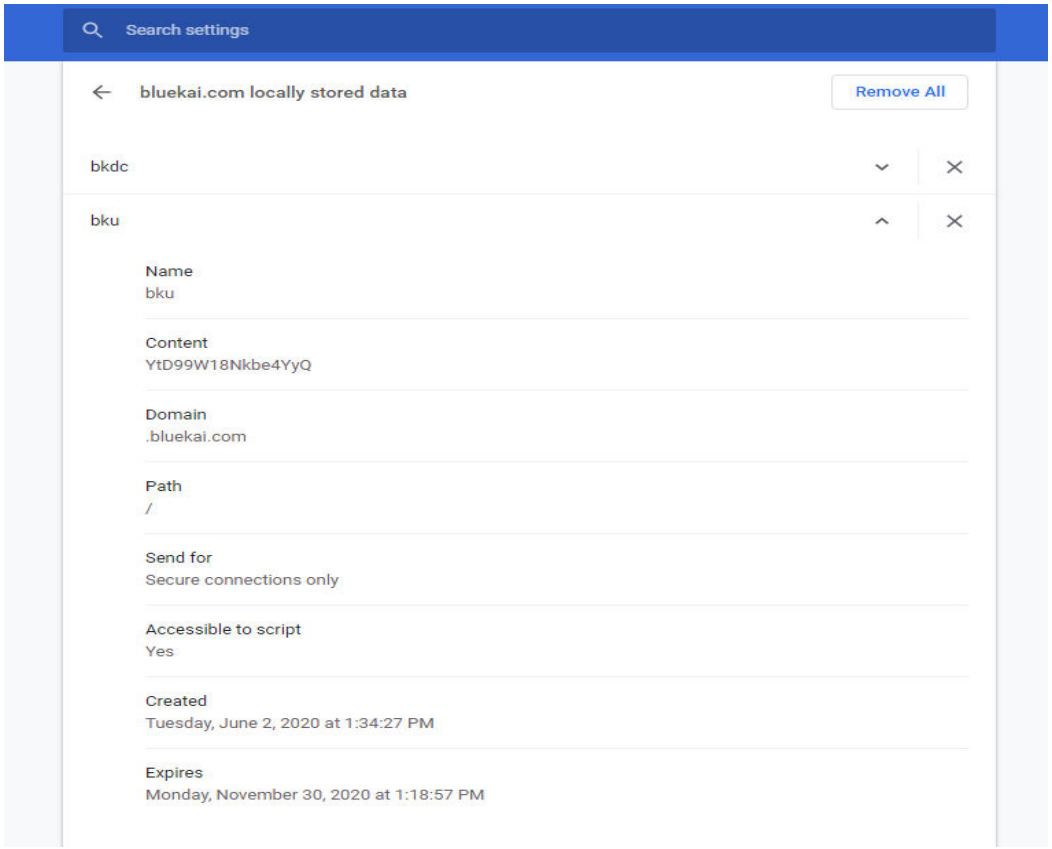
72. However, in the advertising market, cookies are not used for this purpose. Instead, cookies are primarily used to distinguish one Internet user from another and to collect their data. This is done by giving the cookie a unique code (the '**Cookie ID**') that is part of the cookie itself and is assigned to the user of a device (such as a computer or smartphone). Reading the Cookie ID each time that a person visits a website means that the person can be recognised and that his Internet use can be tracked, updated and stored across different websites and applications during the desired period of time. Cookies can also be used to track certain actions on the website, such as clicking on a particular news item or buying a product, and these actions can also be linked to this same Cookie ID. Cookies can be placed both by the website holder itself (for instance, if website www.nu.nl places a cookie when the visitor visits www.nu.nl, this is known as a '**first-party cookie**') or by a third party (for instance if www.oracle.com places a cookie when the visitor visits www.nu.nl, this is known as a '**third-party cookie**').

73. Oracle and Salesforce place cookies via third parties' websites. They do this for thousands of websites, which means that the viewing, listening and buying behaviour, as well as the interactions such as the click-and-search behaviour of persons, can be tracked over a long period of time.

74. The cookies that Oracle places via the websites of its clients have the name 'bku', which is a reference to the company BlueKai. **Exhibit 9** shows an example of a bku cookie. This cookie is placed when a visitor visits (for instance) www.voetbalzone.nl and contains a Cookie ID that Oracle can use to recognise the user, which in this case is 'k9L99B9y3a8aHMQA'. This same Cookie ID is again visible upon a subsequent visit to www.touretappe.nl. In this way, Oracle can track the user across the Internet.

75. Salesforce's DMP service also places third-party cookies, its cookies being known as '_kuid_'. **Exhibit 10** contains an example of a _kuid_ cookie. This cookie is placed when a visit is made to www.nu.nl, for instance. The cookie contains a Cookie ID that Salesforce uses to recognise the user, in this case 'Ne6nmAjL'. The same Cookie ID can be seen again on a subsequent visit to www.buienradar.nl and www.mediamarkt.nl. In this way, Salesforce too tracks the user across the Internet.

76. In the Chrome browser, an Internet user can easily see which cookies are present on his device by going to: chrome://settings/siteData. When a user arrives at a website where Oracle places its BlueKai cookies or Salesforce places its Krux cookies, the following information is displayed in the Chrome list of cookies, for instance:



77. The name of this Oracle cookie is *'bku'*. The domain that can read the cookie is bluekai.com. The cookie was placed on 2 June 2020 and will expire on 30 November 2020. This means the cookie has a lifetime of 150 days. The Cookie ID (called 'YtD99W18Nkbe4YyQ') means that Oracle can always recognize the user.

78. The Salesforce cookie has the name '*_kuid_*'. The domain that can read the cookie is krxd.net. The cookie was placed on 3 June 2020 and will expire on 12 January 2021. This means the cookie has a lifespan of more than 7 months. The Cookie ID, in this case 'NcSjjNF5', means that Salesforce can always identify the user.

79. Cookies are used very extensively in the advertising market. Recent research shows that when an average homepage (the 'landing page') of a website is loaded, 55 cookies are placed. If a person visits additional pages within the same website (for instance by clicking on the heading of an article on a news website) then this number increases to 78 cookies.[53] Research carried out in 2010 on the top 50 most visited websites showed that the average webpage uses 64 independent tracking techniques, including cookies.[54]

80. **Exhibit 11** contains an overview of what happens in the background in the few seconds that it takes to load the homepage of www.nu.nl. The 35-page overview shows not only how all kinds of data are collected but also how the advertising players assign identification numbers to the user, which they later read to link the user with the use made of the website.

81. Cookies are placed on the user's smartphone, computer or other device and can only be read again on that same device. Each cookie makes it possible to recognise the user each time he uses the same device and the same browser. A disadvantage of 'behavioural targeting' is that a fragmented picture of an Internet user is created. After all, Internet users use a range of devices, with thousands of cookies and similar tools - each with their own identifiers - being placed on all these devices.

82. Ad tech companies, including Oracle and Salesforce, have found solutions for this. Oracle and Salesforce assign an identifier to the range of devices that belong to one and the same person, to create a 'cross-device' link between these devices.[55] They may use IP addresses, location data, login data or pattern recognition to do this.[56] AdTech companies also exchange collected information with each other by linking up cookies, this being known as 'cookie syncing'. In this way, the ad tech companies can get the most complete picture possible of a user. Salesforce for instance explains that the location data is used to link up devices:

[53] Cookiebot, *How do website track users?,* 10 July 2020, can be consulted via: https://www.cookiebot.com/and/website-tracking/ and T. Urban, T. Holz, M. Degeling & N. Poholman, '*Beyond the Front Page:* Measuring Third Party Dynamics in the Field', can be consulted via: https://arxiv.org/pdf/2001.10248.pdf, consulted on 4 May 2020.
[54] A. Narayanan & D. Reisman, 'The Princeton Web Transparency and Accountability Project', *Springer* 2017 ([**Exhibit #)**, p. 5., can be consulted via https://lonlon.io/webtap_book_chapter.pdf, p. 5.
[55] https://www.oracle.com/data-cloud/products/data-management-platform/cross-device.html, Oracle purchased the Crosswise company to specialise further in this 'cross-device' linking up; https://konsole.zendesk.com/hc/and-us/articles/215234358-Cross-Device-User-Matching, consulted on 11 August 2020.
[56] Mozilla, *This is Your Digital Fingerprint,* 26 July 2018, can be consulted via: https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint/.

> *'The core of the model is designed to uncover the devices that stay together in various places over long periods of time. To do this effectively there are three important considerations - scale, training, and validation.*
>
> *Scale - Because the success of the model is predicated on seeing lots of devices and how they move over time, it is essential to have massive reach into the device world. With one of the largest device footprints on the planet, Audience Studio has an advantageous position from which to deliver accurate results.'*[57]

83. Oracle uses such services as Crosswise for this, which was one of its acquisitions (see marginal number 50). As Oracle described it at the time of the acquisition:

> *'Crosswise's innovative technology processes over one petabyte of user and device activity data from billions of unique devices every month. By applying advanced data science and proprietary machine-learning techniques to this data, Crosswise constructs a new probabilistic Device Map™ matching multiple devices to individual users in an accurate, scalable and high quality manner.'*[58]

84. Oracle and Salesforce use more than just Cookie IDs to track users. Other IDs are used too to link personal data to a particular person. This may relate to IDs linked to login details, e-mail IDs, device IDs and mobile advertising IDs[59], as well as to IDs that are provided by data partners and clients. This then is what DMPs specialise in, namely in the linking up, organizing and analyzing of data from a wide range of sources.

3.2.2 The collecting of data

85. Oracle states in one of its privacy documents (see also section 4.3.1.1 below) that it collects the following information:

- *unique IDs such as the ID of your mobile device or a cookie ID in your browser;*
- *an ID of a connected device, such as an ID for a smart TV or streaming device (is only used for corresponding purposes in the US);*
- *IP addresses and data that may be derived from IP addresses, such as the geographical location;*
- *data about your device, such as browser, device type, operating system, the presence of or use made of 'apps', and the screen resolution and language preferences;*
- *personal information that has been made unidentifiable, such as e-mail addresses on which a hash processing has been carried out (direct IDs are removed);*
- *demographic information, such as gender, age and income scale, when this information is not linked to information with which you are directly identifiable;*

[57] https://konsole.zendesk.com/hc/and-us/articles/115009397188-Cross-Device-Identity-Management-CDIM-FAQ-, consulted on 11 August 2020.
[58] https://www.oracle.com/corporate/acquisitions/crosswise/, consulted on 23 April 2020.
[59] A Mobile Advertising ID is an ID that is linked to a mobile device. The ID basically acts as a Cookie ID for mobile applications.

- *behavioural data from a computer or device that is connected to the Internet and that you use during your interaction with websites, applications or other linked devices, such as advertisements that you clicked on or that you viewed, websites and content areas, date and time of these activities or the web search action that you used to search a website or to navigate to it.*[60]

86. In other words, it relates to all kinds of data that can be used to distinguish one Internet user from all the others, including an IP address and demographic data that are tied to the unique device ID of the device that the Internet user is using.

87. Salesforce collects similar data. One of its privacy documents (see section 4.3.1.2) refers to the fact that Salesforce collects *'pseudonymized personal data related to that user's visits to the website or mobile app (our Customer's 'Session Data')'*. Session data is explained as follows:

> *'This Session Data may include information about how the user came to the Customer Site and App, which search engines they use, the search terms used to find the Customer Site, their experience on the Customer Site and App, information about how they interact with the Customer Site and App, demographic information that the Customer has collected from that user and other visitors, data from third-party data providers, and information regarding how users interact with advertisements on the Customer Site and App. Additionally, browsers automatically send certain standard information to every website a user visits, such as an IP address, browser type and language settings, access times, and referring website addresses.'*[61]

88. A recent data breach at Oracle gives an impression of the raw data that is used to build up profiles (**Exhibit 12**).[62] TechCrunch states that Oracle's business unit BlueKai continually collects information about Internet users 'behind the scenes' to build up profiles and to constantly enrich these profiles. The raw data that was released by this data breach included data about a German man - including his name, address, telephone number and e-mail address - who had used a debit card to spend € 10 on online bets. This is especially sensitive information, because it contains data that relates to a potential gambling addiction. In other words, it relates to data about health.

> *'Behind the scenes, BlueKai continuously ingests and matches as much raw personal data as it can against each person's profile, constantly enriching that profile data to make sure it's up to date and relevant.*
>
> *But it was that raw data spilling out of the exposed database.*
>
> *TechCrunch found records containing details of private purchases. One record detailed how a German man, whose name we're withholding, used a prepaid debit card to place a €10 bet on an esports betting site on April 19. The record also contained the man's address, phone number and email address.*

[60] Privacy Policy for Oracle Data Cloud, paragraph 4. https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under 4, consulted on 23 April 2020 (also **Exhibit 22.a**).
[61] https://www.salesforce.com/products/marketing-cloud/sfnc/audience-studio-privacy/ (also **Exhibit 23.d**).
[62] Techcrunch, *Oracle's BlueKai tracks you across the web. The data spilled online,* 19 June 2020, can be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).

Another record revealed how one of the largest investment holding companies in Turkey used BlueKai to track users on its website. The record detailed how one person, who lives in Istanbul, ordered $899 worth of furniture online from a homeware store. We know because the record contained all of these details, including the buyer's name, email address and the direct web address for the buyer's order, no login needed.'

89. These aspects of the DMP services of Oracle and Salesforce will be looked at below. However, we will first examine how Oracle and Salesforce create profiles from the information that they collect.

3.2.3 Creating profiles

90. Providers such as Oracle and Salesforce use cookies and similar techniques to collect all kinds of data from many websites, apps and devices. They then enrich this information with information from other sources and then process the collected information automatically. When doing so, they also evaluate particular personal characteristics of Internet users. This is primarily done to analyse and predict personal preferences, interests, behaviour and other characteristics of Internet users. This is known as 'profiling'.

91. Profiles contain information such as gender, town/city of residence, age, number of devices in use etc., as well as more sensitive information that includes information about Internet searches, the websites someone visits, the articles that someone reads and his/her buying behaviour. This information can then be combined and evaluated to derive personal traits, preferences, interests and other characteristics. In this way, a detailed and intrusive picture of the individual in question is built up.

92. Regulatory authorities are rightly concerned about this. The ICO has expressed its concern that privacy rules are being disregarded by the way in which this data aggregation takes place. This British regulatory authority emphasises that this relates to very detailed profiles that are shared with innumerable companies. In its report on this matter, it expresses its concerns as follows:

'We list our concerns - that the creation and sharing of personal data profiles about people, to the scale we've seen, feels disproportionate, intrusive and unfair, particularly when people are often unaware it is happening.

We outline that one visit to a website, prompting one auction among advertisers, can result in a person's personal data being seen by hundreds of organisations, in ways that suggest data protection rules have not been sufficiently considered.'[63]

'The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge.'[64]

[63] ICO Information Commissioner's Office, *Update report into AdTech and real time bidding*, 20 June 2019 (**Exhibit 1)**, p. 4.
[64] ICO Information Commissioner's Office, *Update report into AdTech and real time bidding*, 20 June 2019 (**Exhibit 1)**, p. 23.

93. To create such profiles, the data that Oracle and Salesforce collect is linked to each other as much as possible using a single central ID, this being the ID that links up all the other IDs. Oracle calls this its 'Oracle ID Graph'. Oracle describes its ID Graph as a fundamental technology that drives the Oracle DMP. All the links that Oracle creates are continually validated and scored. This relates not only to the Cookie ID but to other identifiers and to 'massive amounts of IDs' according to Oracle. In addition to its Cookie IDs, Oracle refers to 'login, HH [% sales penetration], email, and mobile ad IDs on a weekly or sometimes daily basis from ID data partners'. The Oracle ID graph can reach 90% of all people who are online in the US and other international markets:

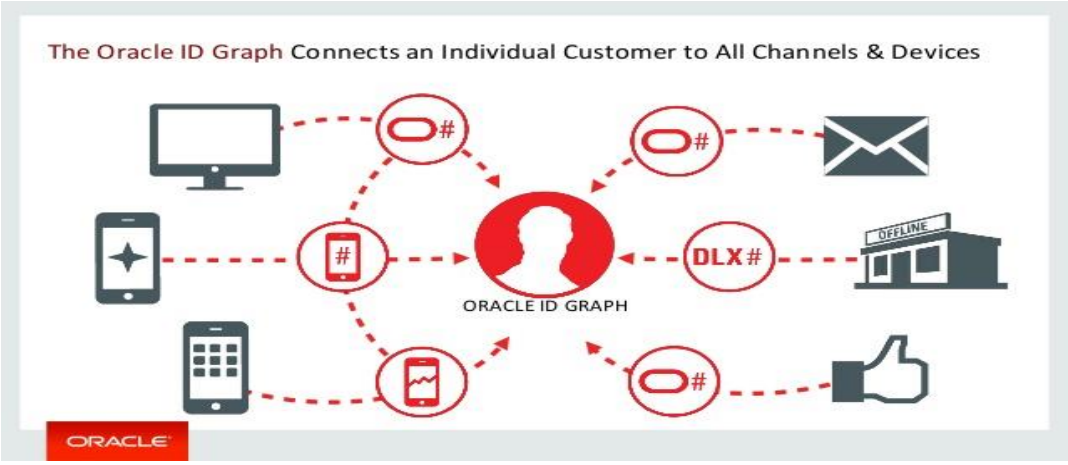
> *'**The Oracle ID Graph, a Foundational Technology That Powers the Oracle DMP**: The Oracle ID Graph establishes and validates connections between IDs that enable the transport of data from one ID space to another, for the purposes of targeting or measurement applications. The Oracle ID Graph is not a product but it is a foundational capability or technology that power the Oracle DMP. All linkages in Oracle ID Graph are continuously validated and scored, which changes dynamically based on a proprietary algorithm to the input. Only the linkages deemed accurate are accepted. Oracle ingests massive amounts of IDs across cookies, login, HH, email, and mobile ad IDs on a weekly or sometimes daily basis from ID data partners. The Oracle ID Graph can reach over 90% of people online in the US and in markets that matter internationally so users can deliver audiences, at scale, and across channels'.*

94. On its website, Oracle states that it places the power of the ID Graph in the hands of the marketeers. Thanks to this unique profile, marketeers have even more options for the precise targeting and analysis of their target group.

> *'The Oracle Data Management Platform's Audience Builder puts the power of the Oracle ID Graph in the hands of marketers. The Audience Builder allows marketers to visualize linkages and build audiences across devices. With enhanced audience segmentation and delivery, Oracle DMP users now have even more options to define exactly who they want to analyze and target by selecting the device ID from the environment from which the data was collected.'*[65]

[65] https://www.oracle.com/data-cloud/products/data-management-platform/cross-device.html, consulted on 23 April 2020.

95. Oracle promotes its ID Graph with the following illustration, for example:



https://www.slideshare.net/BobLewis15/oracle-marketing-cloud-49482488, consulted on 24 April 2020.

96. Salesforce has a similar ID Graph. Salesforce for its part states that this is only available for the American market.[66] Nevertheless, Salesforce too links up data on a massive scale. As stated above, Salesforce markets itself as a specialist in the linking up of different devices that belong to one and the same person, doing so using 'one of the largest device footprints on the planet' (see marginal **82**).

97. In this way, Oracle and Salesforce collect data about the behaviour of users from a computer, tablet or smartphone, as well as from their e-mail, social media and offline data (including in-store purchases). Oracle links up ('syncs') all this data to each other to create a single large-scale data profile of the Internet user, irrespective of which device or application he is using.

98. As part of this process, advertisers use the DMPs to create target groups known as 'audiences'. 'Audiences' are essentially lists of persons who share certain characteristics. Advertisers do this using the data from the DMP, their own data and data from third parties that they can also obtain via another DMP. For example, an advertiser can search for persons who are likely to buy a particular type of product because they are similar to existing clients. These persons constitute the target group.

99. Documentation on the Oracle and Salesforce websites reveals that both parties create target groups as part of their DMP.

100. Documentation from Oracle reveals that clients can use their own data ('first-party data'), data from other Oracle services ('second-party data') and data from Oracle's data partners[67] ('third-party data') to create target groups (**Exhibit 13**):

> *"Digging a little deeper, note that a segment may contain one or more first-party, second-party, and third-party categories. For example, a segment may include*

[66] https://help.salesforce.com/articleView?id=mc_rn_october_2019_dmp_act_seg_ID_graph.htm&type=5, consulted on 11 August 2020.
[67] Data partners (in Dutch: 'gegevenspartners') are the parties whose data is offered by Oracle and Salesforce in their respective data marketplaces. For example, an Advertiser may use Oracle's DMP to utilise data from data partner 'ShareThis'.

users interested in purchasing one or more products or services, users with a specific geographic location or demographics, or any other data category available in the Oracle BlueKai DMP."[68]

101. Oracle then shows an illustration that reveals that with just a few clicks, 'third-party data' from 'Oracle's data partners' and others can be used to create target groups. Oracle then shows how many people are part of the target group, so that these people can be targeted with advertisements.[69]

102. Documentation from Salesforce paints a similar picture. Salesforce markets the 'third party' sources that its own service utilises as follows (**Exhibit 14**):

"*Salesforce Audience Studio has many third-party data options – use the search field or expand the third-party data provider folders to find an appropriate segment.*"[70]

103. Salesforce quotes examples, for instance a target group of men with an income of more than 60 thousand dollars each and another target group comprised of women living in Boston. Salesforce also quotes examples of characteristics that can be used to determine target groups, such as age, educational level, ethnicity, health & fitness, hobbies, marital status, wealth, politics, religion & spirituality and travel. When the DMP service is used to create a target group, Salesforce uses the sources selected to search for persons who come under this target group, so that the advertiser can target this target group.[71]

3.2.4 The enriching of profiles with information from other sources

104. Oracle and Salesforce enrich the information that they have gathered online via their cookies with information from alternative sources. They acknowledge that they also consult offline sources, such as loyalty programmes and surveys, to make the profiles they have created as complete as possible. In addition, they work with a huge number of 'data partners' to enrich the profiles.

105. Oracle also states in one of its privacy documents (see section 4.3.1.1 below for more details) that it collects information from both offline and online sources.

"*Oracle may process certain offline and online information about yourself, including information that originates from publicly available sources or external data suppliers.*

- *Oracle obtains **offline information** about you from its offline partners such as physical stores, supermarkets and their loyalty programmes, payment card brands, catalogue orders and consumer surveys, as well as*

[68] Oracle Create Audience Segments, **Exhibit 13**, also available via: https://learn.oracle.com/ords/launchpad/learn?page=create-audience-segments&context=0:41799:41822, consulted on 22 July 2020.
[69] Oracle Create Audience Segments, **Exhibit 13**, also available via: https://learn.oracle.com/ords/launchpad/learn?page=create-audience-segments&context=0:41799:41822, consulted on 22 July 2020.
[70] Salesforce Segment Builder Guide, **Exhibit 14**, also available on https://konsole.zendesk.com/hc/en-us/articles/217950467-Segment-Builder-Guide, consulted on 22 July 2020.
[71] Salesforce Segment Builder Guide, **Exhibit 14**, also available on https://konsole.zendesk.com/hc/en-us/articles/217950467-Segment-Builder-Guide, consulted on 22 July 2020.

from third parties who may have no relationship with you and who collect offline information from their offline partners.

- ***Online information*** *about you stems from your activities on sites of our online partners, such as advertising agencies and website administrators (including online stores or travel websites). Oracle also obtains online information from third parties who may have no relationship with you and who collect information online using cookies or similar technologies such as pixel tags and device IDs while you are navigating on the Internet and interacting with websites. For more information about cookies and similar technologies that are used in connection with Oracle Data Cloud, please see Section 11 below.*

  Our online Oracle Marketing & Data Cloud data partners are listed in our catalogue, together with an extensive list of our current data suppliers in the EU/EEA. Some of these partners only provide information about persons in specific regions."

106. Oracle can either collect this offline and online information about data subjects itself or else purchase it from third parties, even if the latter have no relationship with the data subject.

107. The term 'offline information' includes phone numbers and online buying patterns:

- *name and residential address, e-mail addresses and phone numbers;*
- *demographic characteristics, if related to other information with which you can be identified;*
- *transaction data from your purchases, when this is linked to other information with which you can be identified;*
- *business information such as the name, size and location of the company where you work and your job title within the company;*
- *data from marketing registration lists, as well as from consumer surveys and public information;*
- *only for the United States: latitude and longitude data that is derived from a physical address.*[72]

108. In addition, Oracle enriches the data with information that it receives from third parties. These third parties are often referred to as 'data partners' (or in Dutch text as 'gegevenspartners'). The catalogue of data partners from which Oracle obtains data consists of approximately 75 companies.[73] A number of these 75 companies are themselves data traders that obtain data from a wide range of sources. The question is whether these numbers are correct. In 2017, Oracle said it had over 1500 data partners (**Exhibit 15**).

[72] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, par. 4, consulted on 23 April 2020 (also **Exhibit 22.a**).
[73] https://www.oracle.com/nl/data-cloud/solutions/data-as-a-service/data-providers.html, consulted on 21 July 2020.

109. Oracle also offers the option of 'partner integrations' or 'media integrations'. Oracle has fully catalogued which identifiers belong to which Internet users, even in respect of the media and applications on which advertisements are displayed.

110. As stated, Oracle emphasises the fact that the DMP acts as an 'enabler' for the digital marketing ecosystem. The system of media integrations Oracle uses means that right from the start it can work with all kinds of media partners. On its website, it refers to having '200 partner integrations' for its DMP:

> *"With the Oracle ID Graph as the foundation, the Oracle DMP can stitch all these different ID sources together to provide better match and scale at bringing data in and delivering data out to the over 200 partner integrations."*[74]

111. The list of integrations includes exchangers, ad networks, DSPs, other DMPs and ad tech parties. According to Oracle, the list includes 'every major media company', including Google, Facebook, Twitter, TikTok, YouTube, Twitter and other data traders such as Lotame, Salesforce, Adobe and AppNexus.[75]

112. Oracle also obtains data via Oracle and Bluekai cookies and uses cookie syncing to exchange information with other data traders that was obtained using cookies. Oracle states the following, for instance:

> *"Oracle and our advertising technology partners use cookies and similar technologies (such as pixel tags and device IDs) to recognise you and/or your devices on and away from various services and devices for the purposes that are defined in the above Paragraph 5."*[76]

113. The data collected and purchased by Oracle includes the following:

a. Cookies that Oracle places on many thousands of websites of Publishers that are clients of Oracle, especially via the 'bku' cookie. Publishers can not only link up this data with Oracle's database but can also sell the data using Oracle's DMP.[77] Research has revealed that out of a selected list of 100 popular websites that are much visited by Dutch Internet users, 28 of these websites place Oracle's cookies (**Exhibit 16**, see also section 3.3). These include news websites nu.nl, ad.nl, trouw.nl, parool.nl, volkskrant.nl, a number of local news websites, sport website voetbalzone.nl, marktplaats.nl and booking.com. On 10 of these 28 websites, cookies are placed before the Internet user has had any interaction with the website (such as clicking on 'I accept cookies'). The research also reveals that the domain placing these cookies is 'bluekai.com' (**Exhibit 16**, see also section 3.3). This means they are third-party cookies that are only read by Oracle. **Exhibit 9** contains an example of such a cookie. This cookie, which bears the name 'bku' and which is placed when a visitor visits www.voetbalzone.nl, contains a Cookie

[74] https://www.oracle.com/data-cloud/products/data-management-platform/, consulted on 17 July 2020.
[75] https://www.oracle.com/data-cloud/solutions/data-as-a-service/media-integrations.html, consulted on 4 August 2020.
[76] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under 11, consulted on 23 April 2020 (also **Exhibit 22.a**).
[77] https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/index.html#UsingBlueKaiIntegrations/becoming_a_data_provider.html%3FTocPath%3DIntegrator%2520Guide%7C6, consulted on 26 April 2020: "*The Oracle Data Cloud enables data providers to activate and monetize their data assets in the Oracle Data Marketplace. To become an Oracle Data Cloud data provider, follow these steps.*"

ID that Oracle can use to recognise the user. This same Cookie ID is again visible upon a subsequent visit to www.touretappe.nl. In this way, Oracle tracks the user across the Internet.

b. Data that Oracle collects via social media buttons such as buttons that can be used to share news articles or other content on websites via Facebook or WhatsApp. Oracle's DMP obtains data for instance from AddThis (an Oracle service) and ShareThis (a third-party service). These are two of the largest providers of social media buttons. ShareThis[78] collects data worldwide via more than 3 million parties such as websites and apps, as well as via more than 1.8 billion cookies and more than 18 billion interactions. The data relates to such areas as travel, pharmaceutical products, retail and finances (**Exhibit 17**).[79] Oracle promotes ShareThis as one of the parties that also obtains data from the EU, which it explains as follows:

> *"ShareThis is the leading source of online behavioural data across the open web. With a global network of 3M publisher domains, the ShareThis network captures shares, searches, clicks, and pageviews, providing a dynamic and comprehensive picture of consumer interest and intent. Marketers can leverage this proprietary, real-time data to better understand their audiences and connect with them in the moments that matter most."*[80]

Oracle's own AddThis buttons are used on more than 15 million websites.[81] These are used to process data from more than 900 million website users and 1 billion mobile users. For each webpage on which AddThis social media buttons are located, Oracle collects up to 30 data points.[82] Both ShareThis and AddThis services provide these buttons free of charge but when doing so say almost nothing about the fact that data is collected when the buttons are used.[83]

c. Data via social media. The extent of this data collection is not clear but Oracle states itself that it obtains data via social media:

> *"Access to more than 700 million social messages daily via feeds from more than 40 million social media and news data sales."*[84]

Oracle also obtains data from Affinity Answers (a third party). In 2019, it stated in this regard that it also obtains data from Affinity Answers about persons in the EU.[85] Affinity

[78] https://sharethis.com/, consulted on 23 April 2020.
[79] Oracle Data Directory 2019 (**Exhibit 17)**, pp. 131-132.
[80] Oracle Data Directory 2019 (**Exhibit 17)**, pp. 131-132.
[81] https://www.addthis.com/, consulted on 23 April 2020.
[82] Oracle Audience Playbook, can be consulted via: https://fliphtml5.com/atnl/kjmi/basic. The Oracle Audience Playbook contains a list of the interest segments that can be accessed using Oracle AddThis. It includes interest in political parties, homosexual films and a person's financial situation. Oracle also states that AddThis is used to collect data from more than 15 million websites worldwide.
[83] https://sharethis.com/ and https://www.addthis.com/, consulted on 26 June 2020.
[84] See the description of Oracle's 'Data as a Service' service in Oracle Cloud – Oracle Data as a Service for Business, can be consulted via: http://www.audentia-gestion.fr/oracle/daas-for-business-2245611.pdf.
[85] Oracle Data Directory 2019 (**Exhibit 17)**, pp.17-18.

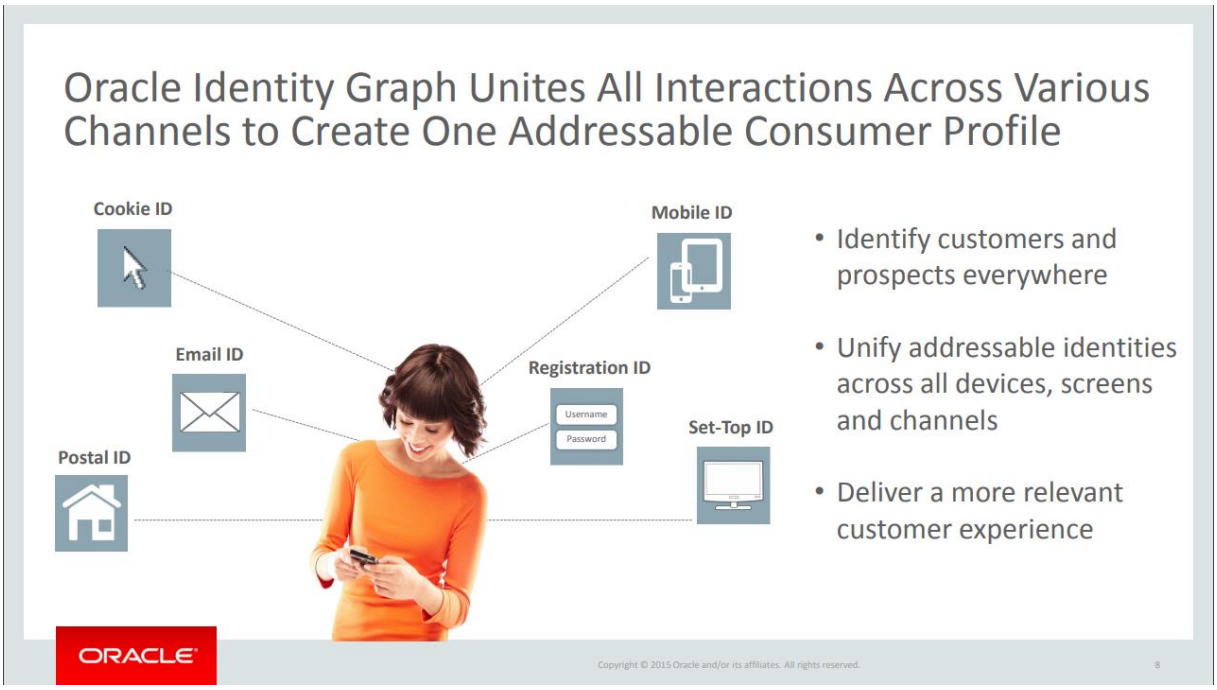
Answers uses data from social media to enrich profiles and to find new clients. This relates to data from more than 400 million social media users.[86]

d. Data that it obtains through exchanges with other data companies using cookie syncing. As revealed by research carried out by Dr. Ahmad Bashir that is discussed below, Oracle obtains data (via cookie syncing) from the following data partners amongst others, even though these parties are not named in the list of Oracle's 'data partners' that Oracle exchanges data with within the European Union:

   i. 'crwdcntrl', which is the domain of Lotame, which is also a DMP and large-scale data trader and 'krxd', the domain of Krux (Salesforce);

   ii. 'id5-sync', which is the domain of ID5, a party that specialises in efficient, large-scale cookie syncing. ID5 makes it possible for numerous invisible parties to link up their cookies with each other with just a single cookie-syncing action.

114. The illustration below shows how all this information is brought together in the Oracle ID Graph. Oracle combines data about the behaviour of users of computers, tablets, smartphones, e-mail, offline data (including in-store purchases) and social media.



https://www.oracle.com/us/assets/general-presentation-2395307.pdf, p. 8, consulted on 24 April 2020.

115. Salesforce enriches its profiles in a similar way. Salesforce too amasses information from offline sources and works together with 'data partners' from whom it obtains information.

116. Salesforce too operates a Third-Party Data Marketplace as part of the DMP with data from a large number of data partners:

[86] Oracle Data Directory 2019 (**Exhibit 17**), pp. 17-18.

*"**Third-Party Platforms***

The Audience Studio Services integrate with and allow users to interact with third-party advertising technology partners, products, services and platforms, including Non-SFDC Applications, websites, products, services and platforms operated by or on behalf of a customer of the Audience Studio Services, whether through a partner of Salesforce or otherwise (collectively 'Third-Party Platforms').

● Customers must enable the Audience Studio Services to access customers' Third-Party Platform accounts if needed to perform the services for the integration selected by customer.

● The Audience Studio Services may access, collect, process, and/or store information or Content from Third-Party Platform accounts (including information otherwise classified as Customer Data under customer's agreement with Salesforce).

● Customers are solely responsible for any content their users or consumers provide to any Third-Party Platform.

[…]

● Available integrations are listed here."[87]

117. The button 'here' refers to lists of data partners that clients can use. This list includes all the major data traders (Google, DoubleClick, Facebook Custom Audiences, Adobe Analytics and Adobe Audience Manager, Oracle Data Cloud, Rubicon, Amazon Advertising, Criteo, Lotame), as well as hundreds of other parties.[88] The list also includes partners who collect data about users' offline lives. This includes data about in-store purchases, credit card use and location data. The list also includes partners that use data from social media use and partners who specialise in combining data. This is similar to the activities carried out by Oracle.

118. The Salesforce website also contains another list of data partners.[89] It is unclear how the two lists relate to each other.

119. Salesforce's data partners include the following:

a. The other major DMPs, namely Oracle Data Cloud, Adobe Audience Manager, Lotame, Neustar and Nielsen.

Salesforce states the following about Lotame:

"Lotame Data Exchange (LDX) data comes from an extensive, global, network of publisher partners and offline data partners. The data consists of self-declared and demonstrated behavioral data from unique publishers, yielding accurate and

[87] https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/audience-studio-notices-and-license-information.pdf, p. 4, consulted on 24 July 2020.
[88] https://konsole.zendesk.com/hc/en-us/sections/206625468-Salesforce-DMP-Ecosystem-Partners,, consulted on 29 April 2020.
[89] https://www.salesforce.com/products/commerce-cloud/partner-marketplace/, consulted on 29 April 2020.

scalable demographic, behavioral interest, and social influencer audience segments. Lotame Data bundles 100% declared and demonstrated - NOT panel-based - data into over 6,000 audience segments across all major verticals (Auto, Travel, Finance, Retail, CPG). Lotame's global reach covers North America, South America, Europe, and Asia."[90]

b. A number of other major data traders that have been investigated in the United States by a Senate committee and the competition authority: Acxiom, Experian, Epsilon, Datalogix (now part of Oracle) and CoreLogic.

It is stated explicitly with regard to Acxiom that the service also covers the Netherlands and also that each week, Acxiom contributes to more than 3 trillion transactions.[91] *Salesforce lists the following subjects (and others) about which Acxiom provides data: age, composition of the family, interests, politics, sport, health insurance, financial situation, good causes (charities etc.), health and fitness, ethnicity and social media.*[92]

c. Payment provider Mastercard Advisors, which delivers data from Mastercard about more than 160 million transactions per hour:

"MasterCard Advisors is the professional services, data & analytics arm of MasterCard Worldwide, the global payment processor.

Leveraging insights drawn from 160,000,000+ transactions an hour generated by over 2.2 billion MasterCard payment cards. MasterCard Audiences allows advertisers the ability to target more effectively by leveraging aggregated past purchase behavior within specific categories (i.e. fine dining, retail, etc.) to identify heavy, frequent and consumers highly likely to spend."[93]

d. Supplier of social media share buttons ShareThis (see marginal 113.b above).[94]

e. Parties that use 'public information', such as Mobilewalla (which also admits to collecting data about 'politics'):

"Mobilewalla provides device-ID based segments for targeting mobile in-app audiences on Android and iOS. Mobilewalla has the IP to make sense of billions of data points daily, which allows hundreds of millions of devices to be classified with high confidence. By associating every device ID with installed apps, lat/long and points of interest, the user is classified into hundreds of demographic and behavioral segments. The company's footprint extends throughout North America, Europe and Asia, covering 20 countries."[95]

---

[90] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under Lotame, consulted on 29 April 2020.
[91] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under Acxiom, consulted on 29 April 2020.
[92] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under Acxiom, consulted on 29 April 2020.
[93] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under MaxterCard Advisors, consulted on 29 April 2020.
[94] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under ShareThis, consulted on 29 April 2020.
[95] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under MobileWalla, consulted on 29 April 2020.

f. Parties such as Placed, Inc. and Factual that specialise in the collection of location data.

Salesforce states the following about Factual:

"Factual is the neutral data company making high quality location data accessible to everyone. Factual's Global Places data is the leading independent data set covering over 85 million local businesses and points of interest in 50 countries and used by 1000s of developers/companies including Apple Maps, Facebook Places, and Microsoft Bing. Factual maps anonymous location data from mobile devices to these places to generate mobile-first location-based audiences to enhance publishers' advertising products.

Factuals Global Places data is built from billions of inputs from millions of sources including user contributions from its network of app clients, relationships with listings management companies and with retail brands, and data from the web. Factual partners with mobile publishers, networks, and ad exchanges to gather anonymous location data from mobile devices, cleans the data using its Location Validation Stack, and then builds location-based audiences tied to mobile IDs."[96]

Documentation from Factual reveals that the Netherlands is one of these 50 countries.[97]

120. Salesforce too uses cookie syncing technology on a massive scale to link up its cookies and the attached data with those/that of other parties, including Oracle, Google, ad exchanges and other data traders.

121. The end result of all this is a gigantic mountain of data that has been obtained from hundreds of parties and combined with data obtained via thousands of websites and apps and with data obtained using synchronisation with the cookies of other data traders. The data relates to the use made of smartphones, laptops, tablets and TVs and relates not just to people's online lives but to their offline lives too. During the takeover of BlueKai in 2014, Oracle noted that it was collecting more than 30,000 data points on each individual and collating them into more than 700 million profiles.[98] In 2017, it claimed it had no less than 2 billion profiles[99] at its disposal, with it even quoting a figure earlier this year of 3 billion profiles that had been collected via 15 million websites.[100] The persons to whom the profiles relate have no idea which data these 30,000 data points relate to.

122. Since DMPs trade large volumes of data via their data marketplaces and also aggregate and combine data, they are often considered to be data traders too.[101]

---

[96] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, under Factual, consulted on 29 April 2020.
[97] Factual, *Knowledge Base; Places; Supported Countries,* can be consulted via: https://developer.factual.com/docs/places-supported-countries.
[98] https://www.oracle.com/us/assets/general-presentation-2150582.pdf, consulted on 23 April 2020.
[99] **Exhibit 15**, news report Oracle Marketing Cloud Teams with Eyeota to Enhance Global Data Offering.
[100] https://www.oracle.com/corporate/acquisitions/crosswise/, consulted on 6 May 2020.
[101] See for instance the report called 'Out of Control' published by the Norwegian consumers' association and available at https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf, p. 37. See also the complaint made by Privacy International, available at https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf.

3.2.5 The use made of profiles for RTB

123. As explained above, RTB is a system where advertisers bid for (advertising and other) space on a website. Basically, this works as follows:[102]

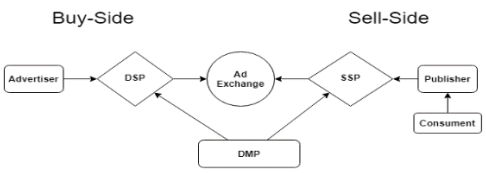
a. The holder of a website[103] (the '**Publisher**') has access to onscreen windows in which he can display specific messages. The content of these windows, such as advertising banners, can be varied, depending on the website visitor in question. In this way, the Publisher can display a different message, depending on the profile of the website visitor. The Publisher offers these windows for personalised content for sale. Publishers use the services of a third party to sell the advertising space on their behalf. This third party is known as a Supply Side Platform or SSP. In addition, many Publishers utilise the services of a DMP to collect data about their visitors, so as to generate additional income from the advertising space.

b. An advertiser ('**Advertiser**'), such as the seller of a product or service, wants to utilise the most interesting space on a website by displaying clickable advertisements or other content. This is why the Advertiser tries to buy the space – such as an advertising bar – that is most likely to generate a purchase. Advertisers use the services of a third party for this, who buys the advertising space on their behalf. This third party is known as a Demand Side Platform or DSP. Advertisers also use a DMP that assesses data about website visitors so as to decide who is most inclined to buy their product, so that the advertisement is then shown to these people.

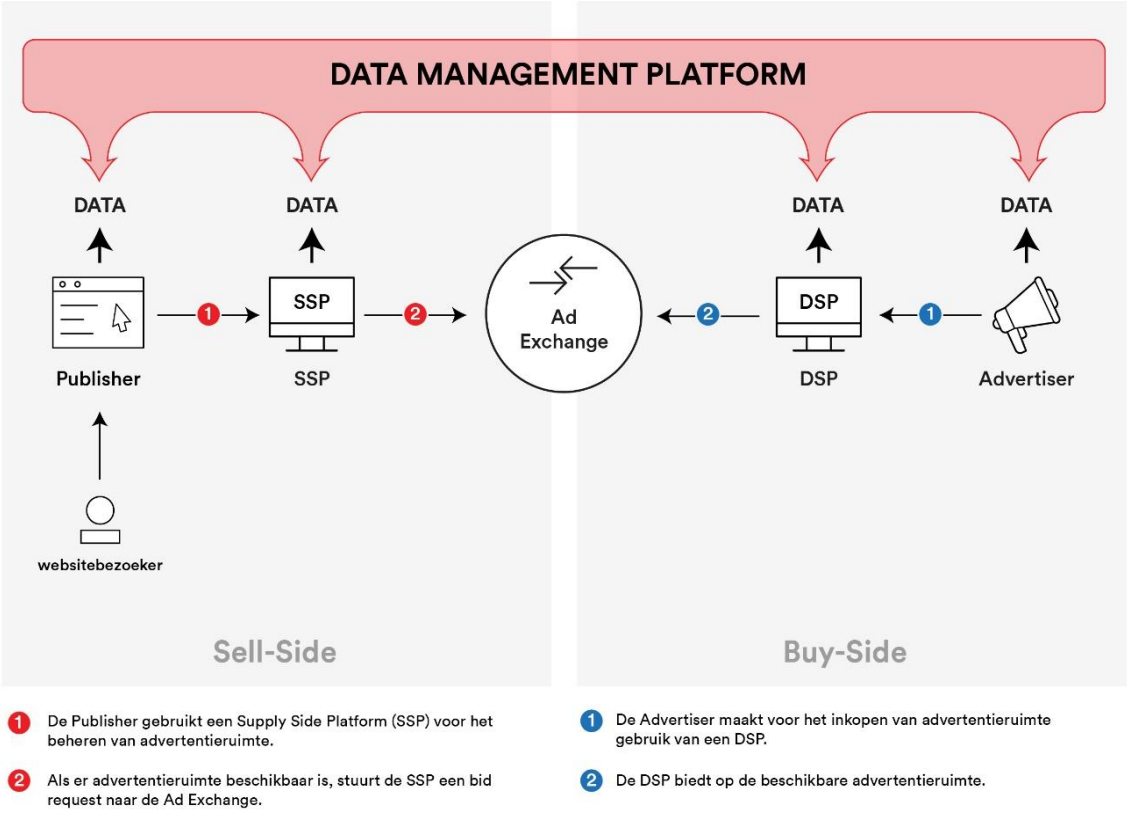
c. When a person loads a webpage on which space is available, the Publisher sends a request that includes the visitor's data (the 'bid request') to one or more auction houses (the 'ad exchanges'). The ad exchanges then send the bid requests to all potentially interested Advertisers, who then bid for the available space in an online auction. Dozens or even hundreds of Advertisers may participate in a single auction for a single advertising bar. The highest bidder gets the space and pays the Publisher. The Publisher then places the advertisement.

124. The ultimate goal here is to induce the website visitor to click on the advertisement. The frequency of this clicking behaviour is known as the 'click-through rate' or 'CTR'. A higher CTR is beneficial for all the commercial parties, namely for the Publisher because he receives a higher price for the advertising space and for the Advertiser because more people buy the product.

125. This may be shown diagrammatically as follows [NB. 'Consument' = Consumer]:



[102] See also a video of a presentation that privacy activist Johnny Ryan held in February 2019 at the offices of the European Data Protection Supervisor about the operation of the RTB system, can be consulted via: https://vimeo.com/317245633./.
[103] RTB is also used to display personalised content in apps or e-mails.



126. To induce the website visitor to click on an advertisement, the content is tailored to the person who will see its content. The various parties use all kinds of data about this person to bring this about.

127. In its report, the British privacy regulator ICO provides information about the data that is sent with bid requests:

> *"The information in a bid request can vary but most include the following:*
>
> - *a unique identifier for the bid request;*
> - *the user's IP address (possibly with the final set of numbers removed, e.g. in Google's Authorized Buyers framework);*
> - *Cookie IDs;*
> - *user IDs;*
> - *a user-agent string identifying the user's browser and device type;*
> - *the user's location;*
> - *the user's time zone;*
> - *the detected language of the user's system;*
> - *the device type (desktop/mobile, brand, model, operating system);*
> - *other information relating to the user (this can vary); and*
> - *information relating to the audience segmentation of the user.*

The above information is personal data where it enables a natural person to be identified, directly or indirectly, from the information itself (alone or in combination) as well as additional information that controllers may possess.

Other information about the user can include:

- *referring sites (where the user came from);*
- *user journey on the site (including mouse cursor movement);*
- *events (scrolling, clicking, highlights, media views);*
- *location;*
- *search queries;*
- *session time;*
- *site behaviour (contextual and thematic preferences to certain topics and pages, interactions such as downloads, transitions to other pages through clicking on advertisements and links); and*
- *demographic data."*[104]

128. All potential bidders thus receive such data about the website visitor – which data they can combine with other data that was previously collected, purchased or otherwise obtained – so that they can bid for (advertising or other) space on the basis of a detailed profile. What's more, these bidders can then do what they like with the data. Neither the Publisher, the ad exchange nor any other involved party now has any more control about what happens with the data once it has been provided to Advertisers.

129. To give you an idea of the size of the RTB market: Index Exchange, which is an ad exchange (i.e. an auction house that deals in advertising space), deals with approximately 50 billion bid requests per day.[105] This means that 50 billion times a day, space on a website or in an application or message is offered for sale and that this offer – including data from the website visitor (the 'bid request') – is sent to the auction house Index Exchange and is distributed amongst dozens or even hundreds of potential bidders who can use the space to display an advertisement or other content to a website visitor. Index Exchange receives no less than 600 billion bids a day in response to the bid requests. And Index Exchange is the smallest of the eight major ad exchanges![106]

3.2.6 Cookie syncing: the linking up of cookies to track Internet users even more closely

130. Ad tech companies use cookie syncing (also known as 'cookie matching') to exchange Cookie IDs with each other. The exchanging of unique indicators is a crucial aspect of RTB, as RTB is not possible without cookie syncing. An average website places no less than 78 cookies on an Internet user's terminal equipment or other device, each of these cookies being assigned a

[104] Information Commissioner's Office, *Update report into AdTech and real time bidding*, 20 June 2019 (**Exhibit 1**).
[105] Index Exchange, *Tour IX's Amsterdam & Frankfurt Data Centers,* 2 July 2019, can be consulted via: https://www.indexexchange.com/tour-ix-amsterdam-frankfurt-data-centers/.
[106] Brave, *Scale billions of bid requests per day,* 2019, can be consulted via: https://brave.com/wp-content/uploads/2019/07/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf.

unique Cookie ID.[107] Cookie syncing ensures that the different parties in the ad tech industry that place cookies can compare these IDs with each other. This is done to exchange information, so that it is clear to all these parties who Internet user 'abc' or 'xyz' is.

131. For instance, when Oracle and Salesforce reciprocally sync their cookies, they are recording the fact that the Internet user that Oracle has assigned Cookie ID 'abc' to is the same person that Salesforce has assigned the Cookie ID 'xyz' to. If Oracle then provides data about person 'abc', Salesforce knows that this relates to person 'xyz'. This process makes it easy for ad tech companies to easily communicate about a person and exchange data about that person. In this way, Cookie IDs are exchanged on a large scale between the website holder, the advertisers, the data management platforms (DMPs) and the other commercial parties involved, so that at all times, all these parties can communicate easily about the same person.[108] This is also how profiles can be linked up with each other.

132. Most of the overview for the loading of the homepage of www.nu.nl (**Exhibit 11**) is devoted to cookie syncing. Pages 5 and 10 for instance list the following links sent by the domain 'acdn.adnxs.com':

https://stags.bluekai.com/site/3085?id=4671557832191386248

https://beacon.krxd.net/usermatch.gif?adnxs_uid=4671557832191386248[109]

133. The code '4671557832191386248' is the code that the placer (in this case AppNexus, another major player in the ad tech market) gives to various companies so that they can link up (i.e. sync) their own cookies with the cookies of AppNexus. As soon as the cookies are linked up, all underlying information about this person can be exchanged. The aforementioned links are addressed to bluekai.com and krxd.net, with bluekai.com being one of Oracle's domains and Krxd being one of Salesforce's. In other words, these links are used to link up AppNexus's cookies with those of Oracle and Salesforce and vice versa. This linking up makes it possible to link up all the underlying information too.[110]

3.3 Investigation into the actions of Oracle and Salesforce

3.3.1 Investigation carried out by Dr. Bashir

134. The Foundation has commissioned research into the activities of Oracle and Salesforce that has been carried out by Dr. Muhammad Ahmad Bashir (**Exhibit 16**). Dr. Bashir obtained his doctorate on the privacy implications of the RTB system and is currently working for the renowned University of Berkeley (USA) and is specialising in technical research into privacy issues relating to the use of (for instance) cookies.[111] He has used a virtual computer with a

[107] Cookiebot, *How do websites track users?,* 10 July 2020, can be consulted via: https://www.cookiebot.com/en/website-tracking/ and T. Urban, T. Holz, M. Degeling & N. Poholman, '*Beyond the Front Page:* Measuring Third Party Dynamics in the Field', can be consulted via: https://arxiv.org/pdf/2001.10248.pdf.
[108] A technical explanation may be found on Clearcode, *What is Cookie Syncing and How Does it Work?,* 15 December 2015, can be consulted via: https://clearcode.cc/blog/cookie-syncing/.
[109] These links are sent by the company AppNexus, which is also a major player in the AdTech market. The links can be found on pages 5 and 10 of the overview for the loading of the homepage of www.nu.nl (**Exhibit 11**).
[110] In many cases, the data partners are not actually named but numbered. See for example p. 4 of the overview for the loading of the homepage for www.nu.nl (**Exhibit 11**):
https://image4.pubmatic.com/AdServer/SPug?partnerID=27&partnerUID=42a75ea7-e1e4-4300-ac31-a6b76c529cb3
[111] See for instance https://cltc.berkeley.edu/about-us/researchers/ahmad-bashir/ and https://www.ahmadbashir.com/.

Dutch IP address to automatically visit websites and to monitor which connections these websites make and which cookies these websites place. To do this, he has used a selection of 100 much-used Dutch websites and visited 6 random pages on each of these websites. This research has allowed Dr. Bashir to map out which popular Dutch websites use tracking technologies from Oracle and Salesforce.

135. Dr. Bashir has analysed which of these 100 websites place the Oracle and Salesforce cookies. Oracle uses the cookie that goes by the name of 'bku' that is placed by the domain bluekai.com, whereas Salesforce's cookies are known as '_kuid_' and are placed by krxd.net. He has also analysed which parties use cookie synchronising technologies to synchronise their cookies via these websites.

136. His research shows that Oracle and/or Salesforce place cookies via 41 of the 100 websites. Oracle places cookies on 28 websites,[112] Salesforce places cookies via 31 websites, and both of them place cookies on the same 18 websites. These include the websites (and others) listed below, the following list also stating which of the 2 parties is placing cookies and the number of *unique visitors* attracted by the website in the month of June 2020.[113]

- Bol.com – Salesforce – 9.97 million
- Buienradar.nl – Salesforce – 8.36 million
- Marktplaats.nl – Oracle and Salesforce – 7.88 million
- Booking.com – Oracle and Salesforce – 2.49 million
- Startpagina.nl – Oracle and Salesforce – 3.12 million
- Mediamarkt.nl – Salesforce – 2.93 million
- Libelle.nl – Oracle and Salesforce – 2.37 million
- News websites:
  - Nu.nl – Oracle and Salesforce – 7.22 million
  - Ad.nl – Oracle and Salesforce – 7.39 million
  - Rtlnieuws.nl – Salesforce – 5.53 million
  - Trouw.nl – Oracle and Salesforce – 2.66 million
  - Volkskrant.nl – Oracle and Salesforce – 3.85 million
  - Parool.nl – Oracle – 2.62 million
  - Indebuurt.nl – Salesforce – 2.45 million
  - gelderlander.nl – Oracle and Salesforce – 2.06 million.

137. Dr. Bashir has also found out the number of websites on which cookies are already placed before consent for this has been given. For Oracle this is 10 websites, for Salesforce this is 12.

138. His research has also identified the parties that Oracle and Salesforce use cookie syncing to link up with (see section 3.2.6 for more information). The research reveals that on the 28 websites on which Oracle cookies were found, Oracle uses cookie syncing with 12 other parties. However, it probably syncs with far more parties than this, because one of the parties with whom Oracle synchronises cookies is the company ID5 (id5-sync). ID5 specialises in effective,

[112] The websites that place cookies before asking for consent are listed here, as are those that place cookies after consent has been given to do so, see annexes 6 and 7 of **Exhibit 16**.
[113] Based on NOBO statistics, available on http://vinex.nl/wp-content/uploads/2020/07/NOBO-Top-50-juni-2020.xlsx.

large-scale cookie syncing. Oracle can use ID5's services to synchronise cookies with innumerable other companies with just a single cookie syncing action. Neither the user nor even Dr. Bashir himself can see which parties this relates to. Oracle also synchronises cookies with the following (and other) parties:

a. 'rubiconproject', the domain of Rubicon Project, which is one of the biggest ad exchanges that in its own words processes advertisements for more than one million websites and for 60,000 mobile applications;[114]

b. 'crwdcntrl', which is the domain of Lotame, which is likewise a DMP and a large-scale data trader;

c. 'krxd', the domain of Krux, owned by Salesforce; and

d. 'spotxchange'; the domain of SpotX, and 'tidaltv', domain of TidalTV, both of which specialise in advertisements in videos.

139. Cookies are already synchronised with 5 parties before the Internet user has given his consent for this. These parties include ID5, Salesforce and Lotame.

140. Salesforce synchronises cookies on 31 popular websites with 23 other parties, with Salesforce cookies being found on these websites too. These include:

a. 'adnxs', which is the domain of AppNexus, a data trader that specialises in organising the exchanging of data;

b. 'bluekai', the domain of Oracle;

c. 'doubleclick', a domain of Google, the largest player in the advertising market;

d. 'everesttech' and 'demdex', both domains of Adobe, which likewise offers a DMP service in which it acts as a data trader;

e. 'openx', 'pubmatic', domains of eponymous parties who specialise in personalised advertisements;

f. 'rubiconproject' and 'casalemedia', which are both ad exchanges;

g. 'spotxchange', 'tidaltv', and 'fwmrm', which all specialise in in-video advertisements (**Exhibit 16**).

For 15 of these 23 parties, cookies are synchronised before the user has given any type of consent for this. These parties include Oracle, AppNexus and Google.

141. Dr. Bashir's research shows that Oracle's and Salesforce's technologies are used on many 'household name' websites that almost all Dutch people visit. This means that almost every Dutch person will come into contact with the DMPs of Oracle and Salesforce. This research also shows that more than just cookies are placed via these websites and that Oracle and

[114] https://rubiconproject.com/.

Salesforce simultaneously link up these cookies with dozens of other parties, including ad exchanges, other DMPs and data traders.

142. **Exhibit 18** provides an overview of the websites that – according to the research carried out by Dr. Bashir (**Exhibit 16**) – use cookies provided by Oracle and/or Salesforce. The overview reveals that most of the websites do not ask for consent in the correct way and/or fail to provide information about the processing of personal data by Oracle and Salesforce (see also sections 4.6.2 and 4.6.3).

143. Column C in the overview reveals the scope of these websites during the month of June 2020 in the Netherlands, as far as is known. Here, use was made of the NOBO programme[115] (the Netherlands Online Scope Research programme) and SimilarWeb. The total number of unique visitors in this month varies from over 2 million visitors that visited degelderlander.nl to almost 10 million that visited bol.com.[116] Websites such as buienradar.nl (over 8 million), nu.nl (over 7 million), marktplaats.nl (almost 7 million) and rtlnieuws.nl (over 5 million) have many unique visitors too.

144. Dr. Bashir has only researched whether Oracle and Salesforce cookies are found on certain websites. However, the processing by parties is not limited to these websites. Many other websites state in their cookie policy that Oracle and Salesforce are partners of theirs that can use the cookies that are placed via their websites or else that they use the services of Oracle and Salesforce in other ways. Both DMPs are named for example in the list of approx. 550 data partners of telegraaf.nl.[117] Funda.nl likewise also names Oracle and Salesforce in a list of approx. 600 ad tech partners. In the month of June 2020, these websites had 5,862,000 and 4,797,000 unique visitors respectively.[118] This means that the scope of the relevant data collection by Oracle and Salesforce is even larger – being in fact many times greater – than would be suspected by the use made of their cookies. All in all, it may be concluded that Oracle and Salesforce collect and process data from almost every Dutch Internet user.

145. Oracle and Salesforce tailor their services specifically to the Dutch market too. In the case of Oracle, those parts of its website that relate to the promotion of its DMP service are available in the Dutch language. The page in question also contains the Dutch contact details for Oracle. The list of Oracle's media integrations can be found on a Dutch-language page too (**Exhibit 19**).

146. This is likewise true for Salesforce. Although there is no Dutch version of the Audience Studio and Data Studio Privacy Policy, all promotional webpages for the sale of the DMP service are available in the Dutch language. Salesforce also provides Dutch contact details and promotes the service by naming Dutch clients who use it. In 2018, major media companies De Persgroep, Sanoma and Telegraaf Media Groep stated that they would start using the Salesforce DMP in

[115] The NOBO is a research programme carried out by VINEX (Verenigde Internet Exploitanten) and the foundation Stichting KijkOnderzoek. Each month, the NOBO catalogues the number of *unique visitors* to the Top 50 most-visited media platforms. 16 of the 41 websites were listed in the NOBO statistics.
[116] http://vinex.nl/wp-content/uploads/2020/07/NOBO-Top-50-juni-2020.xlsx.
[117] Can be viewed by clicking on 'derden' ('third parties') in the cookie banner of https://www.telegraaf.nl/.
[118] http://vinex.nl/wp-content/uploads/2020/07/NOBO-Top-50-juni-2020.xlsx.

the field of 'programmatic advertising' (**Exhibit 20**). In addition, there are several resellers that offer the Salesforce DMP service in the Netherlands.[119]

3.3.2 Viewing Oracle's segments

147. Oracle allows Internet users to view (via datacloudoptout.oracle.com) part of the personal data that has been processed about them. **Exhibit 21** shows such an overview for a Dutch Internet user. The overview contains 11 pages of interest segments and other information. It can be seen for instance how links are made with Google and other ad tech companies such as DataXu, AppNexus, Beeswax and Mediamath. Named interest segments include 'job search', 'fitness', 'fitbit', 'Men's health magazine', skincare product 'Neutrogena', payment providers and interests that include computer games, films, electronic goods and cars. In addition, Oracle appears to be using its 'Oracle Modelling 360' service to assess the person's emotional state, with a reading of 'shocked_EU > 20-30%' being quoted, for instance.

148. In the letter dated 18 June 2020, Oracle states that it only uses four 'data providers', all of whom have to comply with strict criteria. However, the overview provided by Oracle itself reveals that it works with far more 'data providers'. The overview also reveals the existence of a large volume of 'branded data' from ad tech partner Affinity Answers, which specialises in the analysis of social media usage. In 2019, this company was still being referred to as a partner that also provides data from European Internet users.[120] However, Oracle now states that it no longer uses Affinity Answers to collect EU data.[121] Despite this, the overview reveals that Oracle is still processing personal data from European Internet users that it receives from Affinity Answers.

3.4 Data breaches at Oracle and Salesforce

149. As explained above, on their DMPs Oracle and Salesforce collect, process and share large volumes of data about large numbers of people. The risks inherent in this large-scale collection, processing and sharing become painfully evident when the various security issues and data breaches that Oracle and Salesforce have had to deal with in practice are considered. In fact, both parties have suffered multiple data breaches in which large volumes of data were leaked. A few examples are given below:

a. On 19 June 2020, technology website TechCrunch published an article about a data breach related to Oracle's DMP service (**Exhibit 12**).[122] A researcher had gained access to a server and shared data with TechCrunch. The researcher and TechCrunch thus obtained access to billions of data points from an enormous group of data subjects. This included not only names, addresses and email addresses but also data about participation in online gambling for e-sports and payment data.

[119] See for example: https://emark.com/nl/landing/salesforce-dmp/.
[120] See http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf, p. 17.
[121] See https://www.oracle.com/data-cloud/solutions/data-as-a-service/data-providers.html.
[122] Techcrunch, *Oracle's BlueKai tracks you across the web. The data spilled online,* 19 June 2020, can be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).

The researcher and TechCrunch could access the data because the server on which the data was stored was not properly secured and also because no login password was required.

The publication also shows that Oracle blames the unlawful access on incorrect settings used by two customers. It also takes the position that it has taken additional measures to prevent such incidents happening in the future.

According to TechCrunch, the size of the accessible database alone makes this incident one of the largest security breaches this year. [123]

b. In February 2020, an American citizen launched a class action lawsuit based on new Californian privacy regulations following a data breach at Salesforce. Customer data from a clothes shop for children had been unprotected and accessible for almost two months, this relating to names, addresses, credit card data and other data that was then offered for sale on the 'dark web'. The data breach was caused by malware installed on the Salesforce platform.[124]

c. In 2018, Salesforce warned some of its customers that the data they had stored had been accessible to third parties for over a month. This was due to a software error that was Salesforce's fault. Salesforce did not check the traffic to its servers and so could not find out whether and to what extent use was made of the breach.[125]

d. In May 2018, a data breach took place at a start-up company called Apollo. The breach related to more than 200 million contacts (individuals and companies), with a total of more than nine billion data points. Many customers of Apollo had linked their account to Salesforce, allowing the exchange of data between Salesforce and Apollo. For this reason, the Apollo data breach also involved a large volume of Salesforce data.[126]

4. LEGAL FRAMEWORK

4.1 Introduction

150. In the case of the aforementioned activities, Oracle and Salesforce are processing personal data on a large scale and are acting in violation of Internet users' right to privacy. The right to the protection of personal data and the right to privacy are recognised as fundamental rights.

151. Article 7 of the Charter of Fundamental Rights of the European Union (the '**Charter**') contains the general right to privacy. Article 8 of the Charter defines a separate and autonomous fundamental right to the protection of personal data.[127] Article 8(1) of the Charter reads:

[123] Techcrunch, *Oracle's BlueKai tracks you across the web. The data spilled online,* 19 June 2020, can be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).
[124] Law Street, *Salesforce Cloud Data Breach Leaked Thousands of Customers' Information,* 5 February 2020, can be consulted via: https://lawstreetmedia.com/tech/salesforce-cloud-data-breach-leaked-thousands-of-customers-information/.
[125] Bank Info Security, *Salesforce Security Alert: API Error Exposed Marketing Data,* 3 August 2019, can be consulted via: https://www.bankinfosecurity.com/salesforce-security-alert-api-error-exposed-marketing-data-a-11278.
[126] Wired, *A Recent Startup Breach Exposed Billions of Data Points,* 10 May 2018, can be consulted via: https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/.
[127] As does the (amended version of the) TOFEU (the Treaty on the Functioning of the European Union) (in Dutch: the 'VWEU') (*OJEU* 2010, C 83/47), in which the right to the protection of personal data is set out in Article 16.

> *"Everyone has the right to the protection of personal data concerning him or her".*

152. In the second paragraph, five conditions are set for the processing (numbering added by lawyer): "*[The] data must be (1) processed fairly, (2) for specified purposes and (3) with the consent of the data subject or on some other legitimate basis provided for in law. (4) Everyone has the right of access to the data which has been collected about him or her, as well as (5) the right to have it rectified."* The third paragraph requires the setting up of an independent authority to supervise compliance with these rules.

153. The implementation of the Charter in 2019 has ensured that the protection of personal data has taken a very prominent place in the court rulings of the European Court of Justice (the '**CJEU**'). The CJEU has repeatedly confirmed that it is not possible to interpret (lower-level) privacy regulations without first looking at the constitutional background.[128]

154. Within the European Union, the right to data protection was first enshrined in the 1995 Privacy Directive[129], which was implemented in the Netherlands in the Dutch Personal Data Protection Act (the **Wbp Act**).[130] Moreover, in the digital domain, the e-Privacy Directive[131] was adopted, the intention being to augment the Privacy Directive. The e-Privacy Directive aims to ensure a high degree of privacy when communicating over public networks, no matter what technology is used.

155. The General Data Protection Regulation ('**GDPR**') has applied since 25 May 2018; it replaced the Privacy Directive and the Dutch Wbp Act. The EU legislature opted for a regulation instead of a directive, which is why the GDPR's provisions have direct applicability. The GDPR has further strengthened and harmonised the fundamental right to data protection.

156. In the case in question, the conduct of Oracle and Salesforce is assessed in the light of both the constitutional framework, the GDPR and the special provisions in the Dutch Telecommunications Act (the '**Tw**'). It relates to a separate, cumulative assessment.[132] Nevertheless, the GDPR is closely associated with the constitutional context and is an elaboration thereof, as also confirmed by Consideration 1 in the preamble to the GDPR:

> *"The protection of natural persons in relation to the processing of personal data is a fundamental right. By virtue of Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TOFEU) [in Dutch, the 'VWEU'], everyone has the right to the protection of personal data concerning him or her."*

---

[128] See e.g. CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain t. Costeja*), legal ground 38.
[129] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons for the processing of personal data and on the free movement of such data (*OJEC* 1995, L 281-31) ('Privacy Directive').
[130] Act dated 6 July 2000 comprising rules for the protection of personal data (Dutch Bulletin of Acts and Decrees 2000, 302).
[131] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the area of electronic communications (directive on privacy and electronic communications (*OJEC* 2002, L 201/37)). The e-Privacy Directive was amended in 2009 by Directive 2006/24/EC and by Directive 2009/136/EC (*OJEC 2002, L 201/37*).
[132] See also the opinion of Advocate General Saugmandsgaarde dated 19 July 2016 in the consolidated cases C-203/15 and C-698/15, ECLI:EU:C:2016:572, (*Tele2*), item 131.

157. Because the Privacy Directive and the GDPR are largely based on the same concepts, the interpretation of the Privacy Directive by the CJEU or by supranational bodies is also relevant to the interpretation of the GDPR.

158. In this case, Article 11.7a Tw too is relevant to the assessment of the conduct of Oracle and Salesforce. Article 11.7a Tw contains the so-called 'Cookie Law' and constitutes the implementation of Article 5(3) of the e-Privacy Directive.[133]

159. The Dutch Data Protection Authority (the '**DPA**') oversees compliance with the GDPR in the Netherlands. The Netherlands Authority for Consumers and Markets (the '**ACM**') oversees compliance with Article 11.7a Tw for instance. In addition, the DPA monitors compliance with Article 11.7a Tw in respect of the processing of personal data. The European Data Protection Board ('**EDPB**') is a body in which all national privacy regulators from the European Union cooperate in their supervision of the GDPR. The EDPB has succeeded the Article 29 Working Group ('**WG29**').

160. It follows from the factual context that Oracle and Salesforce process personal data – and use cookies – in various ways, including through the following activities:

i. Oracle and Salesforce place cookies equipped with a unique identifier on the Internet user's terminal equipment or other device(s);

ii. Oracle and Salesforce use these cookies and other unique identifiers to collect personal information about the Internet user;

iii. Oracle and Salesforce evaluate the personal characteristics of Internet users, in particular to analyse or predict their personal preferences, interests, behaviour and other characteristics (this is known as 'profiling');

iv. Oracle and Salesforce enrich these profiles and personal data with information from other sources;

v. Oracle and Salesforce provide these profiles to third parties so that they can be used to assess in an online auction how much (if anything) the latter want to bid for advertising space (known as 'realtime bidding');

vi. Oracle and Salesforce link the cookies' unique identifier to the unique identifiers in the cookies of other ad tech parties and thus enable the exchange of data with them (known as 'cookie syncing').

161. It will be argued below in more detail that there are various ways that Oracle and Salesforce are acting in violation of the relevant fundamental rights, the GDPR and Article 11.7a Tw. In particular, the ban on profiling is being infringed, as are the principles of legitimacy, transparency and data minimisation.

[133] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the area of electronic communications (directive on privacy and electronic communications), as amended by Directive 2006/24/EC and Directive 2009/136/EC (*OJEC 2002, L 201/37*).

162. The conclusion is accordingly reached that Oracle and Salesforce are seriously violating the relevant regulatory framework and are acting unlawfully in respect of the persons whose interests the Foundation is representing. In view of the nature, seriousness and duration of the infringement, Oracle and Salesforce are liable for compensation in respect of the data subjects.

163. The violation of the fundamental rights will be looked at in detail, followed by a discussion of the infringement of the GDPR and Tw.

4.2 Violation of Articles 7, 8 and 11 of the Charter

164. Articles 7 and 8 of the Charter are closely interconnected. The right to the protection of personal data is founded on respect for a person's private life. The CJEU has confirmed that data protection by virtue of Article 8 of the Charter is of special importance for the right enshrined in Article 7 of respect for a person's private life.[134] Nevertheless, the implementation of Article 8 of the Charter means that the EU legislature has created an autonomous fundamental right with a specific and far-reaching scope. With its Article 8, the Charter grants a fundamental right *sui generis* for data protection, whereas with the European Convention on Human Rights (the 'ECHR'), personal data is protected by virtue of the general right to the protection of one's private life (Article 8 ECHR).[135]

165. Depending on the nature of the data and the nature of the activities, data collection and data processing can constitute interference by virtue of both Article 7 and Article 8 of the Charter. As Advocate General Cruz Villalon explains in his opinion on the case *Digital Rights Ireland*, a distinction can be drawn between 'ordinary personal data' and information that is more related to a person's private life and to intimacy, in other words that reveals special characteristics of a person's private life. Interference in the first category would primarily concern Article 8 of the Charter, whereas interference in the second category would also infringe Article 7 of the Charter.[136]

166. In the present case, the conduct of Oracle and Salesforce concerns both a particularly serious interference with the right of respect for private life (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter).

167. Creating a gigantic database of data on Internet users, linking databases of third parties thereto, enriching the information, creating profiles, the long-term storage of the data set, all this affects the protection of private life to a particular extent. The mere presence of such a huge data set that can only be created with modern technologies for big data, algorithms and artificial intelligence is already posing a constant threat to private life.

168. In the *Digital Rights Ireland* case, it concerns the retention of a limited number of specific data on the basis of a specific directive that specifies that, in short, Telecom providers store data for the investigation and prosecution of serious crime by competent authorities. This concerns, inter alia, data that are required to trace and identify the source and destination of

[134] CJEU 8 April 2014, case nr. c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), legal ground 53.
[135] See for instance ECHR ruling on 16 February 2000, no. 27798/95, (*Amann t. Zwitserland*), legal ground 65.
[136] Opinion of Advocate General Cruz Villalon dated 12 December 2013, case c-293/12, (*Digital Rights Ireland*).

the telecommunications, so-called traffic data. The CJEU found that from these data "very precise conclusions" are drawn over the private lives of the persons.

> *"Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*[137]

169. In its conclusion, AG Cruz Villalon indicates that the mere retention of traffic data in the *Digital Rights Ireland* case results in a "permanent threat" of the right to the protection of privacy and a "feeling of being controlled".[138] This perfectly constitutes an interference of the fundamental right that Article 7 of the Charter protects. The CJEU adds to this that also the access of the competent national authorities forms an additional interference with that right.[139] The fact that data are stored and used later, gives rise to the feeling amongst the persons involved "that their private lives are the subject of constant surveillance", according to the CJEU.[140] The communication of personal data to a third party also constitutes an interference with Article 7 of the Charter.[141]

170. In this case, it is not only about the retention or communication of personal data, but also about the exchange, enrichment and ongoing and daily collection of an almost infinite amount of data, that exposes special and sensitive characteristics about the personal lives of individuals. It also involves data processing that does not serve the legitimate interests of the government, in particular the competent investigating authorities, but of the purely commercial interests of thousands of parties that are active in the *AdTech* industry.

171. All this obviously forms an interference with Article 7 of the Charter.

172. As the present case concerns the large-scale processing of personal data, Article 8 of the Charter is also affected in the core. Article 8 of the Charter is particularly affected, inter alia, by the placing of cookies equipped with unique identifiers, the exchange of Cookie IDs in the context of cookie syncing and the dissemination of profiles among countless commercial parties in relation to RTB. That applies the more since the data subjects have no idea that their profile is being sold to the highest bidder, let alone what all those hundreds of parties – that have not placed the winning bid but have received the profile – do with their profiles during an auction.

173. In the *Tele2* case, the CJEU ruled that the retention of traffic data also affects the way in which users of electronic communication means make use of their communication tool. The CJEU stresses that therefore, the national legislation at issue that imposes the obligation to retain traffic data should not only be assessed against Articles 7 and 8 of the Charter, which the Swedish and English courts mentioned in the preliminary questions, but also the fundamental

[137] CJEU 8 April 2014, case c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), paragraph 27.
[138] Conclusion of AG Cruz Villalon of 12 December 2013, case c-293/12, (*Digital Rights Ireland*), point 72.
[139] CJEU 8 April 2014, case c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), paragraph 35. See also CJEU 16 July 2020, C -311/18, ECLI: EU:C:2020:559, (*Schrems II*), paragraph 170.
[140] CJEU 8 April 2014, case c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), paragraph 37.
[141] See CJEU 16 July 2020, C -311/18, ECLI:EU:C:2020:559, (*Schrems II*), paragraph 171.

right of freedom of expression that is protected by Article 11 of the Charter.[142] The CJEU calls this fundamental right "one of the essential foundations of a pluralist, democratic society, and [is] one of the values on which (...) the Union is founded".[143]

174. This right is also affected in the core in the present case. After all, the data processing that is the subject of this case can lead to people becoming averse to the use of the main communication tool of our time, the Internet. After all, its use is currently only possible if the Internet user accepts that he is constantly being monitored and that a profile of him is being developed and maintained on the basis of which he is presented with advertisements, which are appropriate to his specific character traits. In particular, the freedom to gather information is affected, which is part of the freedom of expression. This is especially true when the Internet user cannot access information if he does not accept that he is being segmented and monitored, inter alia, by means of "cookie walls".

175. The activities of Oracle and Salesforce thus form a severe interference in the fundamental rights that are protected in Articles 7, 8 and 11 of the Charter. The Foundation can make a direct claim on this for the benefit of the Claimants. The fundamental rights from the Charter operate in horizontal relationships. The CJEU has acknowledged this several times.[144]

176. Under Article 52(1) of the Charter, restrictions on the rights recognised in the Charter must be provided for by law and respect the essence of it. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.[145] In this case, this means in practice that:

- The activities of Oracle and Salesforce must have a legal basis;
- The activities of Oracle and Salesforce respect the essence of the rights recognised in the Charter;
- The activities of Oracle and Salesforce are necessary in order to pursue an objective of general interest, or are necessary to protect their rights and must actually be appropriate to pursuing that objective or protecting those rights;
- The activities of Oracle and Salesforce are proportionate, in a democratic society, to the objective pursued.[146]

177. The conduct of Oracle and Salesforce meets none of these requirements.

---

[142] CJEU 21 December 2016, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, (*Tele2*), paragraph 92.
[143] CJEU 21 December 2016, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, (*Tele2*), paragraph 93.
[144] See inter alia CJEU 8 April 1976, case 43/75 (*Defrenne*), CJEU 12 July 2011, case C-324/09, ECLI:EU:C:2011:474 (*L'Oréal / eBay*), CJEU 24 November 2011, case C-70/10, ECLI:EU:C:2011:771 (*Scarlet/SABAM*). See also CJEU 27 March 2014, case C-314/12, ECLI:EU:C:2014:192 (*UPC Telekabe*l), CJEU 29 January 2009, case C-275/16, ECLI:EU:C:2008:54 (*Promusicae*) and CJEU 19 February 2009, case C-557/07 (*LSG / Tele2*).
[145] CJEU 21 December 2016, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, (*Tele2*), paragraph 94.
[146] Cf. conclusion of AG Saugmandsgaardoe of 19 July 2016 in joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:572, (*Tele2*), point 132.

178. Firstly, it holds that the actions of Oracle and Salesforce are not based on a national law, let alone a European Union directive, as was the case in the *Digital Rights Ireland* and *Tele2* cases. They cannot invoke a legal basis that permits interference with rights that "itself define[s] the scope of the limitation on the exercise of the right concerned".[147] On the contrary, Oracle and Salesforce justify their actions solely on the grounds that these fall within the strict conditions of the GDPR and Tw. In particular, Oracle and Salesforce rely on exceptions or limitations in the legislation, which must be interpreted strictly according to the established case law of the CJEU.[148] As will be shown in the review of the activities of Oracle and Salesforce against the GDPR and Tw, they violate a multitude of basic principles and provisions of the GDPR and Tw. The activities are therefore not based on a sufficiently accessible and foreseeable legal basis that protects properly against arbitrariness, as the criterion "provided for by law" requires.[149]

179. Secondly, it holds that the actions of Oracle and Salesforce affect the essence of the relevant fundamental rights in the core. As indicated above, it is a particularly large and severe intervention in the fundamental rights. After all, the fact that Internet users have no or insufficient knowledge of the offending practices, could give them the feeling that their private life "is being constantly monitored", also according to the CJEU in the *Tele2* case. [150]

180. Thirdly, it holds that Oracle and Salesforce do not perform their operations for the benefit of a general interest. In the *Digital Rights Ireland* case, AG Cruz Villalon writes in its conclusion that the "retention" of data at issue in that case should never exist and, where it does, would therefore require the existence of very compelling reasons of general interest.[151] Well now, in this case there is no question of any general interest. Oracle and Salesforce conduct their operations, including data storage, purely for their own commercial interests and the commercial interests of third parties.

181. Neither can Oracle and Salesforce invoke a special right that provides for the protection of their activities. Insofar as they were to invoke freedom of expression, it holds that this fundamental right only protects advertising to a limited extent. Article 7(4) of the Constitution even excludes commercial advertising from the constitutional protection of freedom of expression. From the established case law of the ECHR, it follows that "commercial speech" enjoys less protection and the Member States have a wide "margin of appreciation" to set limits to it.[152] Freedom of expression offers no protection whatsoever to the multitude of operations of Oracle and Salesforce, considered in conjunction, within the ecosystem of online marketing.

182. In any event, the fundamental rights that the Foundation invokes in this case prevail in the weighing up of these fundamental rights.

183. Fourthly and lastly, there is the requirement that the activities of Oracle and Salesforce should be proportionate to the intended legitimate purpose within the meaning of Article 52 of the Charter. Your court does not need to examine this requirement, as it has already been

[147] See CJEU 16 July 2020, C -311/18, ECLI:EU:C:2020:559, (*Schrems II*), paragraph 175.
[148] CJEU 21 December 2016, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, (*Tele2*), paragraph 89.
[149] Cf. conclusion of AG Saugmandsgaardoe of 19 July 2016 in joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:572, (*Tele2*), points 134-154.
[150] Cf. CJEU 21 December 2016, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, (*Tele2*), paragraph 100.
[151] Conclusion of AG Cruz Villalon of 12 December 2013, case C-293/12, (*Digital Rights Ireland*), point 144.
[152] See, inter alia, ECHR 20 November 1989, case 10572-83, (*Markt Intern v. Germany*), paragraph 33.

established above that the actions of Oracle and Salesforce pursue no legitimate purpose and neither can they invoke an own fundamental right that must be protected. Nevertheless, in the following we explain that the actions of Oracle and Salesforce are not proportionate as referred to in Article 52 of the Charter.

184. It should be noted that the principle of proportionality goes beyond proportionality as a general principle for action in the Union (within the meaning of Article 5(4) of the Treaty on European Union) and is specifically proportionality as a "constitutive condition for any limitation on fundamental rights".[153] To this end, it is required that the exceptions to the protection of personal data remain within the limits of the "strictly necessary". According to established case law of the CJEU, restrictions should include clear and precise rules on the scope and application of the exception, which impose minimum requirements, so that those whose data is collected, enriched, exchanged, stored and sold have sufficient guarantees that their personal data are effectively protected against the risk of abuse.[154] In the recent *Schrems II* case, the CJEU indicates that:

> *"The need for such safeguards is all the greater where personal data is subject to automated processing (...)."*

185. Oracle and Salesforce do not give such guarantees or safeguards. It is absolutely unclear to the average Internet user what information is collected concerning him, for what purposes or for what period. He does not know how his profile is compiled, with whom his profile is shared and how advertisers make offers to him based on his profile. The data are also insufficiently protected, as is shown by the data breaches described in the factual framework.

186. To the extent that "behavioural targeting" may be a legitimate purpose, the manner in which Oracle and Salesforce have set up the process is completely out of proportion. It is unnecessary to collect, enrich, exchange, store and sell the personal data of Internet users on a daily basis in order to create online advertising. Targeted advertising can also be done in other ways. Advertisements can also be focused on the interests of the reader, depending on the content of the article. This is called contextual advertising.[155] The New York Times, among others, has switched to this form of advertising as a result of the GDPR, and its advertising revenues are still increasing.[156]

187. In January 2020, STER Advertising also stopped using cookies to provide advertisements and switched to contextual advertising on the websites of the NPO (Dutch Foundation for Public Broadcasting). STER Advertising published an extensive survey on this and concluded, inter alia, that contextual advertising provides an online sales increase of over 50% compared with advertising based on personal data.[157]

---

[153] Conclusion of AG Cruz Villalon of 12 December 2013, case C-293/12, (*Digital Rights Ireland*), point 133.
[154] See CJEU 16 July 2020, C -311/18, ECLI:EU:C:2020:559, (*Schrems II*), paragraph 176.
[155] Kobler, *Study of Effects of Contextual Targeting on News,* can be consulted on: https://kobler.no/contextual-insights/.
[156] Digiday, *After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue,* 16 January 2019, can be consulted on: https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.
[157] STER Advertising, *A future without advertising cookies? It can be done!*, p. 17.

188. Other privacy-friendly alternatives are available so that websites have the ability to generate revenue using advertisements, without the large-scale trade in data that is inherent to the RTB system.[158]

189. In view of the foregoing, Oracle and Salesforce violate the relevant fundamental rights. As noted in the introduction to the legal framework, the GDPR and Tw partly form a further elaboration of the fundamental rights discussed above. The GDPR and Tw will therefore also have to be interpreted in the light of the protection of fundamental rights that the Union Legislator intends to protect with these regulations. Before dealing with the specific violations of the GDPR and Tw, we will first explain below that the GDPR and Tw apply in the present case.

4.3 Applicability of the GDPR and Article 11.7a of the TA

4.3.1 Processing of personal data

190. The GDPR applies to the *processing* of *personal data*. The person to whom personal data relates is called the *data subject*. Oracle and Salesforce do not dispute that personal data are processed. That is evident from the privacy documentation published on their websites (**Exhibits 22 and 23**).

4.3.1.1 Oracle's privacy documentation

191. Oracle describes its processing of personal data in a series of seven privacy documents.[159] The DMP service comes under Oracle's 'Data Cloud' and is in particular described in the Oracle 'Privacybeleid voor [Privacy Policy for] Oracle Data Cloud' (**Exhibit 22.a**) and the 'AddThis Privacy Policy' (**Exhibit 22.b**).

192. The Privacy Policy for Oracle Data Cloud appears to relate to all Oracle Data Cloud and Marketing Cloud services, including the DMP service. The AddThis Privacy Policy relates to data that is collected via the social media buttons that Oracle provides under the name AddThis. This data is used in the DMP service. In addition, Oracle has an "Oracle general privacy policy". Herein it describes, inter alia, the processing of data of its website visitors and customers. The general privacy policy of Oracle does not seem to apply to the DMP service, but because it has been drawn up in very general terms, we cannot rule out that that is the case.

4.3.1.2 Salesforce's privacy documentation

193. The manner in which Salesforce processes personal data must be derived from various documents. The Dutch website contains links to three "privacy statements" (**Exhibit 23.a**):

a. The full Privacy Statement (**Exhibit 23.b**);
b. A message about the Privacy Shield Certification; and
c. A data processing addendum FAQ.

[158] Medium, *Blockchain & Advertising – New Solutions to Old Problems,* 28 June 2018, can be consulted on: https://medium.com/trivial-co/blockchain-advertising-new-solutions-to-old-problems-e7fcbbc16b85.
[159] https://www.oracle.com/nl/legal/privacy/ and https://www.oracle.com/legal/privacy/, consulted on 14 July 2020.

194. In addition, the website includes a summary of the most important points from the full Privacy Statement (**Exhibit 23.a**).

195. The full Privacy Statement (**Exhibit 23.b**) only contains a few parts that refer to the DMP activities as described in this writ, namely:

a. The inclusion of 'advertisement cookies' in the list of types of cookies that Salesforce uses, without any indication of the websites on which it does this, with the description:

> *"Advertisement cookies track activities on websites in order to obtain useful information on the interests of a visitor and to tailor direct marketing to him/her.*
>
> *We sometimes use cookies that are provided by ourselves or by third parties in order to display advertisements for our products on devices that you use, these products in our opinion being ones you may be interested in, as well as to get the latest data about how our advertisements are performing. These cookies collect information for instance about the browser you have used to visit our websites.*
>
> *Salesforce also enters into contracts with third parties' advertisement networks, which third parties collect IP addresses and other information from web bugs on our websites, from e-mails and from third parties' websites. Advertisement networks track your online activities over time and on various websites or via other online services by collecting device and usage data by automated means, including by using cookies. These technologies can recognise you on the various devices you use. When we use third parties' advertisement networks, we require them to limit their data processing to only that which is necessary to provide us with the requested advertising services."*[160]

b. From an unsubscribe option for targeted advertisements from / via Salesforce Audience Studio:

> *"Click here to unsubscribe yourself from targeted advertisements that are provided by Salesforce Audience Studio to ourselves and to third parties."*[161]

c. From an unsubscribe option for targeted advertisements from / via Salesforce DMP:

> *"Click here to unsubscribe yourself from targeted advertisements that are provided by Salesforce DMP to ourselves and to third parties. However, please bear in mind that if you block or delete cookies and similar technologies that are used on our websites, you may not be able to fully benefit from the websites."*[162]

[160] https://www.salesforce.com/nl/company/privacy/full_privacy/, under 4.2 (also attached as **Exhibit 23.b)**.
[161] https://www.salesforce.com/nl/company/privacy/full_privacy/, under 4.3 (also **Exhibit 23.b)**.
[162] https://www.salesforce.com/nl/company/privacy/full_privacy/, under 4.4 (also **Exhibit 23.b)**.

196. A Dutch Internet visitor who visits the Salesforce website[163] is automatically redirected to the Dutch page,[164] which is why he basically only sees the aforementioned information when he clicks on "Privacy Statement". However, much more information is provided on the English-language version of the website, thanks to the latter's privacy documentation[165] (**Exhibit 23.c**). This page includes such documents as one called 'Salesforce Audience Studio Privacy Policy' (**Exhibit 23.d**)[166] that may be found under the button 'Resources in respect of how we protect our customer's data as a processor'. This provides further information about the processing associated with the DMP service of Salesforce. The Salesforce Audience Studio Privacy Policy does not make clear whether it applies exclusively or in addition to the full privacy statement.

197. Other information about the DMP service of Salesforce is available on English language websites of Salesforce that are aimed at Salesforce customers, such as the Trust and Compliance Documentation page of Salesforce (**Exhibit 23.e**).[167] This documentation is not easy to find for the average Internet user.

4.3.1.3 Oracle and Salesforce acknowledge that they process personal data

198. In the above-mentioned documentation, Oracle and Salesforce acknowledge that they process personal data in the context of the DMP service. In its letter of 18 July, Oracle also confirms that it collects personal data (**Exhibit 5**). It distinguishes the data that it – in its own words – collects from "direct identifiers", but in this Oracle does not want to take the position that it does not processes any personal data. Neither is that evident from the letter.

199. Oracle and Salesforce dispute mainly, or at least seem to dispute, that they should be regarded as a controller in respect of the data processing.

200. For the sake of completeness, in the following we will nevertheless substantiate that the information collected by Oracle and Salesforce qualifies as "personal data" and that the actions they perform with the data should therefore be regarded as "processing", to which the GDPR applies.

4.3.1.4 Personal data

201. Article 4(1) GDPR defines the concept of *personal data* as follows:

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

[163] https://www.salesforce.com, accessed on 14 July 2020.
[164] https://www.salesforce.com/nl/?ir=1, accessed on 14 July 2020.
[165] https://www.salesforce.com/company/privacy/, accessed on 14 July 2020.
[166] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/ (also **Exhibit 23.d**).
[167] https://trust.salesforce.com/en/trust-and-compliance-documentation/audience-studio-and-data-studio/ (also **Exhibit 23.e**).

202. The present case, as indicated in the factual framework (paragraph 3.2.2), concerns, inter alia, the following information and data:

a. Data to identify the Internet user, such as a Cookie ID or another online identifier;

b. IP address(es);

c. Location data;

d. Information about the user, such as other websites the user has visited, actions he has performed on websites (such as clicking on an article) and data that are derived from it directly or indirectly, such as gender, age, place of residence, purchasing history, income, occupation, interests and preferences.

The above-mentioned data are indicated in the following by "**Cookie IDs and associated information**".

203. When looking at the different parts of the personal data definition, it also appears that Cookie IDs and associated information fall within this definition. After all, this concerns:

a. information;

b. relating to;

c. an identified or identifiable natural person.[168]

At a, it concerns information

204. In the *Nowak* case, the CJEU confirms that from the words "any information" in the definition of personal data it must be inferred that the Union Legislator intended to give a broad meaning to this term, which extends to any type of information, "not only objective but also subjective, in the form of opinions and assessments".[169] The Cookie IDs and associated data are information. Information can be objective or subjective. Interests and preferences also fall within the concept of information.

At b, relating to

205. Personal data are distinguished from other data or information in that they relate to a person. Cookie IDs and associated information relate to and are about a person, namely a consumer. Information can also be about a person if, for example, it concerns an object that is owned by a person (e.g. the value of a property), or processes or events. Consideration should be given to the content, purpose or result of the information to assess whether the information is about a person.[170] In this case, all information collected and processed by Oracle and Salesforce is designed to obtain the broadest possible profile of an Internet user. All information thus relates to a person.

[168] Working Party Article 29, Opinion 4/2007 on the concept of personal data, 20 June 2007, WP136 ('WP136 Definition of personal data'), p. 6.
[169] CJEU 20 December 2017, C/434-16, (*Nowak*), ECLI:EU:C:2017:994, paragraph 34. This case was delivered by applying the term "personal data" from Directive 95-46.
[170] WP136 Definition of personal data, p. 10-11.

At c, an identified or identifiable natural person

206. The person to whom a Cookie ID and associated information relates is not in all cases an "identified person". After all, in most cases, this information does not directly and immediately reveal who the natural person is who visited a website.

207. There is a person who can be identified, directly or indirectly (through a third party), and thus an "identifiable person". According to Article 4(1) GDPR, a natural person is deemed identifiable who can be identified directly or indirectly, in particular by means of an identifier. As examples of an identifier, this article refers, inter alia, to an identification number, an online identifier and elements that characterise the identity of that person.

208. Cookie IDs and the other identifiers that are used by Oracle and Salesforce (see under 3.2.1) are such online identifiers. After all, these identifiers have no other purpose than to identify Internet users on the Internet so that they can be shown the right advertisement.

209. In the *Planet49* case, the CJEU confirmed that placing a cookie with a unique number, should be considered as processing personal data, which, incidentally, was acknowledged by Planet49.[171]

210. That Cookie IDs and associated information relate to data about an identifiable person, also follows from the interpretation of the Advocate-General in the *Breyer* judgment of the CJEU:

> *"56. The person to which those particulars relate is not an 'identified natural person'. The date and time of a connection and the numerical address from which it originated do not reveal, directly or immediately, the identity of the natural person who owns the device used to access the website or the identity of the user operating the device (who could be any natural person).*
>
> *57. However, in so far as a dynamic IP-address helps to determine — either alone or in conjunction with other data — who is the owner of the device used to access the website, it may be classified as information relating to an 'identifiable person'."* [172]

211. That identification can take place through online identifiers, such as Cookie IDs, is further emphasised in recital 30 of the GDPR:

> *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*

212. WG29 also expressly considers that a Cookie ID is personal data:

> *"When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of*

[171] CJEU 01 October 2019, C-673/17, ECLI: EU:C:2019:801 (*Planet49*), paragraph 45.
[172] Conclusion of AG Campos Sánchez-Bordona of 12 May 2016 in case C-582/14, ECLI:EU:C:2016:779 (*Breyer*).

> *users of a certain computer even when dynamic IP addresses are used[11]. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned."[173]*

213. The CJEU emphasises in this regard that from the fact that the EU legislator uses the term "indirect", it can be inferred that for data to qualify as personal data, it is not necessary that this data in itself permits identification of the data subject. Moreover, it is not required that all the information on the basis of which the data subject can be identified, rests with one and the same party. As a result, dynamic IP addresses, for example, can be classified as personal data.[174] Nor is it relevant whether identification actually occurs.[175]

214. On "behavioural advertising", a process of which the services that Oracle and Salesforce offer form a part, WP29 considers that collecting IP addresses and cookie IDs is intended to distinguish individuals from each other and is information about a person, used to influence that person. In this connection, WG29 also refers to the possibility of linking profiles to other information concerning the data subject.

> *"The Article 29 Working Party notes that the behavioural advertising methods described in this Opinion often entail the processing of personal data as defined by Article 2 of Directive 95/46/EC and interpreted by Article 29 Working Party[22]. This is due to various reasons: i) behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. In other words, such devices enable data subjects to be 'singled out', even if their real names are not known. ii) Furthermore, the information collected in the context of behavioural advertising relates to, (i.e. is about) a person's characteristics or behaviour and it is used to influence that particular person[23]. This view is further confirmed if one takes into account the possibility for profiles to be linked at any moment with directly identifiable information provided by the data subject, such as registration related information. Other scenarios that can lead to identifiability are mergers, data losses and the increasing availability on the Internet of personal data in combination with IP addresses."[176]*

215. Besides Cookie IDs and other online identifiers, Oracle and Salesforce collect and process all kinds of data on Internet users, including the data listed above (under paragraph 3.2.2). All kinds of data about the data subject are also derived from this (directly or indirectly), such as gender, age, place of residence, purchase history, income, occupation, interests and preferences. The overall profile, which consists of collected and derived data, includes data that, in combination with each other, could only apply to one individual.[177] This is also

[173] Working Party Article 29, Opinion 1/2008 on the concept of personal data and search engines, 04 April 2008, WP148 ('WP148 Search engines'), p. 9.
[174] CJEU 19 October 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer*), paragraph 44 and in a similar sense CJEU 29 July 2019, C-40/17 (*Fashion ID*), ECLI:EU:C:2018:1039, paragraphs 26-27.
[175] WP136 Definition of personal data, p. 15-16.
[176] Working Party Article 29, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP171 ('WP171 Behavioural Advertising'), p. 9.
[177] Ministry of Justice and Security, Guide to the General Data Protection Regulation, January 2018, 108 130, p 25.

necessary for the ultimate purpose for which the profiles are compiled; showing an advertisement that matches the characteristics and preferences of one person.

216. The purpose of Oracle and Salesforce is to be able to distinguish Internet users from each other and to make targeted offers to these Internet users, based on their personal characteristics and interests. The purpose is to obtain an image of the highly personal and individual characteristics of the Internet users in order to persuade them to make a purchase or other behaviour. Information that because of the content, purpose or effect serves to evaluate and assess a person should qualify perfectly as personal data. In the *Nowak* case, the CJEU ruled for example that examination answers must be classified as personal data, inter alia, because the collecting of answers "is to evaluate the candidate's professional abilities".[178]

217. Finally, a profile can often be directly associated with a data subject via one or more of the items of data contained in it. Consider, for example, linking a telephone number or IP-address (in the profile) to a name via the telephone or Internet provider.[179]

218. The fact that the Cookie IDs and the associated information that Oracle and Salesforce process relate to personal data, is evident in view of the foregoing.

219. Insofar as Oracle and Salesforce would argue that through pseudonymisation, there is no question of personal data, the following applies. There is pseudonymisation when data are linked to a pseudonym, such as a number, rather than for example the name of the data subject. However, in pseudonymisation, that pseudonym is still traceable to an identified or identifiable person. For that reason, it holds that with the use of pseudonymisation, there are still personal data. However, pseudonymisation can generally be regarded as a necessary security measure, because pseudonymised data can be less easily abused by third parties (see also marginals 514 and further). This does not, however, affect the applicability of the GDPR.[180]

220. Finally, there is also personal data on the grounds of article 11.7a TA, as will be discussed in more detail below (Section 4.3.2.2).

4.3.1.5 Processing

221. Article 4(2) GDPR defines the term "processing" as follows:

> *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"*

222. All actions that can be carried out in relation to personal data, from the first moment that data is collected to its removal, fall under the concept of processing.

[178] CJEU 20 December 2017, C/434-16, (*Nowak*), ECLI:EU:C:2017:994, paragraph 38.
[179] Ministry of Justice and Security, Guide to the General Data Protection Regulation, January 2018, 108 130, p 25.
[180] See also Working Party Article 29, Opinion 5/2014 on Anonymisation Techniques, 10 April 2014, WP216 ("WP216 Anonymisation Techniques").

223. In short, the actions that Oracle and Salesforce carry out in respect of personal data consist of (See Section 3.2):

a. The collection of data through cookies, other online identifiers and from other sources;

b. The coupling to each other, combining and enriching of the data;

c. The analysis and evaluation of the data and the addition of derived information;

d. Storage in the DMP database;

e. The making available of the data for the RTB process.

These actions must be regarded as processing for the purposes of the GDPR.

224. Furthermore, Oracle and Salesforce process the personal data in an automated fashion, so that the processing is subject to the material scope of Article 2 GDPR.

225. Moreover, in the processing, certain personal aspects of Internet users are evaluated, in particular with the goal of analysing or predicting personal preferences, interests, behaviour and other characteristics of Internet users. This way of processing personal data is considered in Article 4(4) GDPR to be profiling. In the facts it has already been set out what extended profiles are established in this way, and what they say about individuals (see in particular Sections 3.2.3 to 3.2.5 inclusive).

226. That the processing can be considered profiling, makes it necessary to consider processing in general as more far-reaching, and that additional obligations apply in order to safeguard the interests of data subjects. These will be discussed in the following (where relevant) when dealing with the infringement of the GDPR and Tw (Section 4.6).

4.3.2 Article 11.7a Tw

4.3.2.1 Applicability to Oracle and Salesforce

227. Besides the processing of personal data, the practice of Oracle and Salesforce qualifies as storing information over an electronic communications network or obtaining access to information in the peripherals of a user, within the meaning of Article 11.7a of the Tw. After all, Oracle and Salesforce place cookies on the peripherals of users.

228. Oracle takes the position only to use first party cookies, which would mean it does not place the cookies itself, but its customers. However, research shows that when visiting a large number of popular websites visited by the Dutch, cookies are placed by an Oracle domain (**Exhibit 16** and **Exhibit 9,** see also marginal 74 and Section3.3.1). That means those cookies are not placed and read by Oracle customers, but by Oracle itself.

229. Salesforce also places third-party cookies, and does not deny this either. The fact that Salesforce places third party cookies is also evident from **Exhibit 16 and Exhibit 10** (see also marginal 75 and Section 3.3.1).

230. The practice therefore falls within the scope of article 11.7a TA, that, in short, requires prior information and consent for placing and reading cookies.

4.3.2.2 Presumptive evidence for tracking cookies

231. In addition, article 11.7a(4) Tw includes presumptive evidence. On this basis, the use of cookies to collect, combine or analyse data on the use of various online services, so that the data subject can be treated differently (so-called tracking cookies), is considered to be the processing of personal data.

232. Articles 11.7a(1) and (4) of the Tw read:

> *"1. Without prejudice to the provisions of the General Data Protection Regulation, storing or obtaining access by means of an electronic communications network to data stored in a user's peripheral equipment is only allowed on condition that the user concerned:*
>
> *(...)*
>
> *4. An act as referred to in the first paragraph, which has the purpose of collecting, combining or analysing data on the use of various services of the information society by the user or subscriber, so that the user or subscriber in question may be treated differently, is suspected to be processing personal data."*

233. The presumptive evidence in paragraph 4 of the Tw has been added because of concerns about the privacy implications of third-party cookies and cookies that collect, combine and analyse surfing habits, interests and other data of Internet users for commercial purposes.[181] This is precisely the core of the present activities of Oracle and Salesforce. After all, the Oracle and Salesforce cookies are placed via a large number of websites, and upon visiting a website, they pass on information about user activity to Oracle and Salesforce. This allows Oracle, Salesforce and their customers to follow the behaviour of data subjects on all those websites. They collect, combine and analyse data on the behaviour of data subjects, and then use that information in order to be able to treat data subjects differently. That falls perfectly under the presumptive evidence of article 11.7a(4) Tw. So also under the Telecommunications Act, the practices of Oracle and Salesforce must be considered as the processing of personal data.

4.4 Accountability

234. As noted above, Oracle and Salesforce seem to dispute that they must be regarded as the "controller" in respect of the data processing described above, at least with respect to parts of their activities.

235. In its letter of 18 June 2020, Oracle indicates that it is only the (independent) controller in respect of part of its DMP service. In its letter, Oracle calls this service Audience Data Marketplace ("ADM"). Oracle calls this service "optional" for its customers. Its DMP however has little or no independent value without the service which it calls ADM. Oracle indicates that

[181] *Parliamentary Papers II,* 2010/11, 32 549, 39.

with ADM, the data it collects via cookies are linked with data from other sources. It is these data that it then sells to advertisers in the RTB process. The distinction that Oracle tries to make here does not exist in fact. The ADM service is part of the DMP service. It is not, or hardly possible, to exploit the DMP service of Oracle commercially without ADM. Oracle itself endorses this in its commercial documentation (see marginal 966.b).

236. Strangely though, in its privacy documentation, Oracle also takes a different view. Oracle certainly describes itself therein as controller. [182]

237. In the Oracle Data Cloud Privacy Policy, that deals specifically with the DMP service, it designates Oracle Corporation and Oracle America, Inc. as controllers for the data processing:

> *"Oracle Corporation and Oracle America, Inc., with their registered address at 500 Oracle Parkway, Redwood Shores, CA, 94065, United States, are responsible for the processing of your personal data within the context of this Privacy Policy."* [183]

238. In the AddThis Privacy Policy (which is only available in English), the following is stated in respect of the controller for the data processing:

> *"Oracle Corporation and its affiliated entities are responsible for processing AddThis Data described in this Privacy Policy. A list of Oracle entities is available here. Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country."* [184]

239. The list of Oracle entities for the Netherlands refers to Oracle Nederland B.V. Since AddThis is part of its DMP, with this information Oracle is also saying that Oracle Nederland B.V. too plays a role in the provision of the DMP service. Incidentally, Oracle's general privacy policy contains a similar provision (in Dutch):

> *"Oracle Corporation and its affiliated entities are responsible for the processing of your personal information as described in this Privacy Policy. To learn more, please go to the list of Oracle entities and select a region and country to see the registered address and contact details for the Oracle entity (entities) in each country."* [185]

240. In its privacy documentation, Salesforce does not indicate clearly how it qualifies its role. It appears to designate itself on the English-language page [186] of the Audience Studio Privacy Policy merely as processor. That only follows from the fact that it has included this Privacy Policy under the heading "Resources in respect of how we protect our customer's data as a processor" (Lawyer's underlining).[187]

---

[182] The privacy documentation was published on: https://www.oracle.com/nl/legal/privacy/, consulted on 14 July 2020.
[183] Oracle Data Cloud Privacy Policy, under "3. Who is responsible for your personal data", see https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 14 July 2020 (also **Exhibit 22.a**).
[184] Privacy Policy for AddThis, under "3. Who is responsible for your personal data", see https://www.oracle.com/nl/legal/privacy/addthis-privacy-policy.html, consulted on 14 July 2020.
[185] Oracle's general privacy policy, under "3. Who is responsible for your personal data", see https://www.oracle.com/nl/legal/privacy/privacy-policy.html, consulted on 14 July 2020.
[186] https://www.salesforce.com/eu/company/privacy/, consulted on 22 July 2020.
[187] It should be noted that Dutch Internet users are not redirected to this English-language privacy page.

241. In the Audience Studio Privacy Policy, however, Salesforce indicates nowhere whether it is controller or processor for the processing operations. Moreover, the Dutch Internet user is only directed to a page where this document is not listed (for this, see marginal 196).

242. The full privacy statement on the Dutch website of Salesforce states:

> *"1. Responsible Salesforce entity*
>
> *"Salesforce is the controller of your Personal Data as described in this Privacy Statement, unless stated otherwise.*
>
> *This Privacy Statement does not apply insofar as we process Personal Data in the role as processor or service provider on behalf of our customers, including when we offer our customers various cloud products and services whereby our customers (or their affiliated enterprises): (i) make their own websites and applications which run on our platforms; (ii) sell or offer their own products and services; (iii) send electronic communications to others; or (iv) collect, use, share or process Personal Data in another way via our cloud products and services.*
>
> *To gain extensive privacy information relating to a Salesforce customer, or an affiliated enterprise of a customer, who uses Salesforce cloud products and services as controller, please contact our customer directly. We are not responsible for the privacy or data security practices of our customers, which may vary from those set out in this Privacy Statement. See also Section 10.3 below for further information."*

243. Nowhere in the privacy statement is it mentioned that Salesforce is not a controller for the processing associated with the DMP service, or that it only processes personal data in this context in the role of processor or as a service provider on behalf of its customers. Thus it gives the impression that it is the controller. This impression is further reinforced by the fact that in the same statement, it does refer to the DMP service on some points (see marginal 195).

244. Insofar as Oracle and Salesforce take the position that they are no "controller" in respect of certain aspects of their services, or at least they make that suggestion, with this Oracle and Salesforce want to argue that they do not need to fulfil many important obligations of the GDPR, inter alia, the obtaining of consent for the data processing (Article 7 of the GDPR), transparency obligations (Article 12 of the GDPR), data minimisation (Article 5(1)(c)) and taking appropriate technical and organisational measures (Article 24 of the GDPR).

245. Insofar as the position of Oracle and Salesforce is that with respect to (some of) the activities they perform, they should only be regarded as "processor", this is incorrect. In the context of the data processing as described above, they certainly qualify as a "controller", as will be explained in the following.

4.4.1 The "controller"

246. Article 4(7) of the GDPR defines the controller as follows.

> *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; […];"*

247. The controller plays a fundamental role within the framework of the GDPR and it is therefore of great importance to appoint him. The controller is, inter alia, accountable for demonstrating his compliance with the principles regarding the processing of personal data (Article 5(2) of the GDPR).

248. The controller must be distinguished from the "processor", which only processes personal data for the benefit of the controller (Article 4(8) of the GDPR). The processor may only process personal data on the basis of written instructions from the controller. The processing by a processor must be governed by a specific agreement (Article 28(3) of the GDPR).

249. The controller is, in short, the one who decides *why* and *how* personal data are processed. [188]

250. Article 4(7) of the GDPR distinguishes between determining the "purpose of" and the "means for" the processing.

251. Determining the purpose is relevant due to the fact that processing is only lawful if [data is] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Article 5(1)(b) GDPR). This does not mean, however, that the person who defines the purposes within the meaning of Article 4(7) GDPR also always defines lawful purposes. It is clear from Article 4(7) GDPR that it concerns the one who "defines" and not "lawfully defines" the purpose and means.

252. Regarding the question as to who is the one who "defines", the European Data Protection Supervisor ("EDPS") indicates the following:

> *"How can this be assessed in practice? In order to evaluate the 'factual influence' of a controller over the processing operation, the entirety of the factual elements should be evaluated, by answering the questions 'why is the processing taking place', 'who initiated the processing' and 'who benefits from the processing'."*[189]

253. It is therefore not only important why processing takes place and who took the initiative, but it is also important who benefits from the processing.

254. The term "means" in Article 4(7) of the GDPR refers not only to the technical and organisational manner in which personal data are processed. The term also refers to the manner in which the processing is carried out (the "how" of the processing). In this context, it

[188] Working Party Article 29, Opinion 1/2010 on the concepts of "controller" and "processor", WP169, p. 15 (WP169 The concepts of "controller" and "processor").
[189] European Data Protection Supervisor ("EDPS"), 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725', p. 7 (Note: It is true that these guidelines do not relate directly to the GDPR, but to related legislation in which the concepts of "controller" and "processor" have the same meaning.).

is relevant, inter alia, to determine who is the one who defines which personal data are processed, who defines which third parties have access to the personal data, and when the personal data are erased.[190]

255. It follows from recital 74 of the GDPR that the responsibility and liability of the controller must be defined for any processing of personal data that is carried out by or on behalf of him:

> *"The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."*

256. In its opinion 1/2010, the WG29 indicates that the responsibility is demonstrated by the *factual* influence that the actors have in determining the purpose and means of the processing of personal data.[191] The concept of controller is a "functional concept".

257. The contractual responsibilities are just an indication regarding the actual role fulfilled by the parties.[192]

4.4.2 Broad interpretation

258. From the case law of the CJEU, it follows that the concept of "controller" should be interpreted broadly, also taking into account the objective of the GDPR to safeguard a high level of data protection. [193] The EDPS confirms that this broad interpretation of the CJEU also serves the objective of avoiding a lack of responsibility, thereby ensuring that data subjects have the guarantee of effective and complete protection.[194]

259. In the *Wirtschaftsakademie* case, the CJEU determined that the person who creates a "fan page" on Facebook should be regarded as a (joint) controller. In this case, it was Facebook that placed a cookie on the computer of the person who visited the fan page. Facebook thus collected data for its behavioural targeting advertising system.[195] The fan page administrator obtained anonymized statistics on website visits from Facebook. It could be concluded from this what were the characteristics and profile of visitors to the website, for example regarding age, gender, interests and online purchasing.[196]

---

[190] Ibid, p. 16.
[191] WP169 The concepts of "controller" and "processor", p. 9.
[192] Conclusion of AG Bot of 24 October 2017 in case C-210/16, ECLI:EU:C:2017:796 (*Wirtschaftsakademie Schleswig-Holstein*), par. 60.
[193] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraph 66; CJEU 10 July 2018, case C 25/17, (*Jehovan todistajat*), paragraph 66; CJEU 05 June 2018, C 210/16 (*Wirtschaftsakademie Schleswig-Holstein*), paragraph 28; CJEU 13 May 2014, C -131/12, ECLI: EU:C:2014:317 (*Google Spain and Google*).
[194] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13. See also CJEU 05 June 2018, case C 210/16, ECLI: EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), paragraph 42.
[195] Conclusion of AG Bot of 24 October 2017 in case C-210/16, ECLI:EU:C:2017:796 (*Wirtschaftsakademie Schleswig-Holstein*), par. 4.
[196] CJEU 05 June 2018, case C 210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), paragraphs 34 and 37.

260. The holder of the fan page was regarded as (joint) controller because, inter alia, he enabled Facebook to place cookies and because he was better able to determine his provision of information thanks to the statistics. The fact that he himself had no access to personal data did not detract from this, according to the CJEU (legal ground 42).

261. In the *Jehovan todistajat* case, the CJEU considered that the community of Jehovah's Witnesses jointly with the individual Jehovah's Witnesses (members) was controller because the community organises, coordinates and encourages religious preaching activities. For this definition of joint responsibility, the CJEU considers it unnecessary that the community has access to the data or that it instructs its members in writing.[197]

262. In the *Fashion ID case*, the CJEU determined that the person who activates a Facebook "Like" button on his website, must be regarded as a (joint) controller. This button is installed by creating a hyperlink to Facebook. When visiting a website that contains the button, an automatic connection is made to the Facebook servers and the website visitor's personal data is sent to them, regardless as to whether he or she has clicked and regardless as to whether he or she has a Facebook account.[198]

263. Whoever activated the "Like" button on his website, was regarded by the CJEU as a controller because he thereby enabled Facebook to collect personal data and was aware of the same.[199] By installing the "Like" button, together with Facebook, the website owner determined the means for the processing of personal data. After all, if the button had not been installed by the website owner, the personal data would not have been processed.[200] The purposes were also established jointly, according to the CJEU, now that the website owner, thanks to the "Like" button, reaps commercial advantage by optimising the advertising for his products through increasing visibility on Facebook.

264. In the case law discussed above, the parties concerned always took the position of being merely processors. According to the CJEU, wrongly. In two of the three cases, it is ruled that the party concerned is joint controller with Facebook. Facebook's role in these cases seems similar in many ways to that of Oracle and Salesforce. Nevertheless, the parties agreed that Facebook primarily determined the purpose and means of the data processing.

4.4.3 Oracle and Salesforce are controllers

265. In the present case, it is also Oracle and Salesforce that should primarily be identified as controllers.

266. From the factual framework it follows that Oracle and Salesforce process personal data in various ways (see Section 3.2). First, it holds that they place cookies on the consumer's peripherals. In the second place, a direct link is created between the cookies thus placed, and the DMP of Oracle and Salesforce. Via this link, Oracle and Salesforce collect, inter alia, the unique Cookie IDs, IP-addresses, data on online purchases and data about the browser. Using different identifiers, Oracle and Salesforce create an "ID Graph" or digital fingerprint to

[197] CJEU 10 July 2018, case C 25/17, (Jehovan todistajat), paragraph 75.
[198] CJEU 29 July 2019, case C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraphs 26 and 27.
[199] CJEU 29 July 2019, case C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraph 75.
[200] CJEU 29 July 2019, case C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraphs 78-79.

connect various unique identifiers to each other. This information is then, thirdly, enriched with information obtained from other sources. Fourthly, on the basis of this, profiles are compiled. Fifthly, Oracle and Salesforce make these profiles available to advertisers who compete in the RTB process to buy advertising space on websites that are visited by consumers. Finally, in the context of RTB, links are made with third-party cookies by means of cookie syncing. These actions are carried out automatically by means of software.

267. It is Oracle and Salesforce that have independently decided to process personal data in this way. It is also Oracle and Salesforce that have determined the results and effects of the data processing. Oracle and Salesforce determine what personal data is collected, from which data subjects, how long the data are stored, who has access to the personal data and how the data processing is secured.

268. It is Oracle and Salesforce that provide the crucial means to collect personal data and to identify consumers, namely the cookies and DMP. It is Oracle and Salesforce that can recognise users on all websites that make use of their technologies. Oracle and Salesforce follow or track the user over the Internet, inter alia on the basis of the Cookie ID that they give to their cookies. It is Oracle and Salesforce that create the link between the data collected via the laptop, tablet, mobile phone, work computer and even on the Internet user's offline life. It is Oracle and Salesforce that exchange Cookie IDs on a large scale with other parties that are active in the RTB process, so that all these parties can always recognise each other's Internet users and exchange data. Without offering the DMP, no collected information could be interlinked, enriched, analysed and shared. Oracle and Salesforce do this for their own commercial interests, namely to enrich the data they obtain and to exploit them commercially by making them available to third parties. Naturally, Oracle and Salesforce know all this.

269. Moreover, from the factual framework it follows that Oracle and Salesforce offer their customers and/or partners a large number of means with which they determine the "how" of the data processing operations (see marginal 64). This concerns, inter alia, a software platform that is constantly being developed and maintained for the benefit of collecting, storing and enriching data and developing and maintaining algorithms to identify one data subject and track his activities across multiple devices. It is Oracle and Salesforce that develop algorithms with the aim of turning the different datasets into profiles and interest segments. It is Oracle and Salesforce that are developing search tools that help Oracle and Salesforce customers to find specific audiences or interest segments.

270. For an advertiser or website owner, it is child's play to integrate Oracle and Salesforce services. With just a few clicks of the button or by adding a few lines to the website's code, a website owner can ensure that cookies are placed through his websites. The DMP then does the rest of the work, including the placing of the cookies, the reading of the cookies and the collection of data. Customers can access a clear DMP dashboard that allows them to link their own data and that of third parties. In addition, they make known which audiences they prefer to show advertisements based on personal information.

271. From the above it follows that Oracle and Salesforce determine the purposes and means of the data processing operations.

272. As stated earlier, in its letter of 18 June 2020, Oracle is however of the opinion that it should be regarded as a "processor" regarding its DMP service (**Exhibit 5**). In other words, Oracle takes the position that it does not determine the "why" and "how" of data processing. That is a remarkable position for a party that describes itself as an "enabler" of online marketing. According to Oracle, it is its customers and/or partners that qualify as controllers. From the foregoing, it is evident that this is not correct. It is Oracle that takes the initiative for the data processing, determines the means thereto and has the greatest commercial interest therein.

273. Oracle puts the cookies on end-user devices and reads them out. It states that there are only "first-party" cookies that are supposedly placed by the Publisher itself, but research shows that Oracle itself places the cookies from its own domain (**Exhibit 16**). Even if this were not the case, then it is still true that it is Oracle that supplies the software or code for the cookies. It is also Oracle that has arranged the cookies such that the collected data are automatically included in the DMP database. Moreover, it is Oracle that chooses to apply cookie syncing. It is also Oracle that determines the means to secure (access to) personal data.

274. In its Audience Studio Privacy Policy, Salesforce acknowledges that it collects data for its DMP about, inter alia, site visits from consumers, which search engines they use, the search terms they use, demographic information and IP addresses.[201] Salesforce indicates, however, that it is its customers, advertisers, who determine whether this data is collected. Salesforce thus ignores the fact that it defines the means for its customers to do this.

275. Salesforce even indicates that its customers that use the Salesforce data partners, are themselves responsible for the use of such data:

> *"● Customers are solely responsible for any content their users or consumers provide to any Third-Party Platform.*
>
> *● Customers are solely responsible for any information accessed by their users, consumers or any third party from any Third-Party Platform."*[202]

276. Using such data is for Salesforce customers no more than pressing the button (see marginals 102 and further). The data have then, however, already been made available through the Salesforce platform. This making available of such data through its platform therefore falls within the responsibility of Salesforce. Note also that Oracle *does* regard itself to be controller for the same service (at Oracle classified as ADM).

277. Moreover, Salesforce also indicates that it determines independently whether various devices belong to the same user and stores that information.[203] Salesforce also acknowledges that the data stored on its DMP is enriched with, for example, geolocation data provided by third parties "*in order to better target advertisements, to enable Customers to better understand*

[201] Salesforce Audience Studio Privacy Policy (**Exhibit 23.d**).
[202] Audience Studio Notice and License Information (**Exhibit 23.f**), under "Third Party Platforms".
[203] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under 'How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform', consulted on 22 July 2020 (also **Exhibit 23.d**).

users across multiple computers and devices, and for ad delivery and reporting purposes".[204] From the foregoing it follows that Salesforce is a controller for the DMP service.

278. That the position of Oracle and Salesforce that they are not controllers is untenable, is also evident from the fact that they do not merely follow instructions from third parties in respect of the data processing. It is also Oracle and Salesforce that determine the basis on which the data are processed (namely, on the basis of consent). Oracle even gives data subjects the opportunity to withdraw their consent. It is also Oracle and Salesforce that determine storage periods and to whom a request for access may be sent under Article 15 GDPR.

279. To the extent that it would be otherwise stipulated in a processor agreement, it holds that not the legal agreements but the actual practices are decisive in determining the controller. Moreover, the contractual documentation of the parties does not make it clear either whether Oracle (**Exhibit 24**) and Salesforce (**Exhibit 25**) see themselves as processor or controller in the context of their DMP service.

280. From the case law discussed above, it follows that several parties may be joint controllers.[205] This also follows from Article 4(7) GDPR. It is important in this context whether there are multiple parties that influence the determination of the purpose and means of the processing, and also whether there are multiple parties that have a commercial interest in the processing.[206]

281. Article 26 GDPR states that when several parties are jointly controller, they mutually establish their responsibilities under the GDPR transparently. In particular, those in respect of the information obligations under Articles 13 and 14 of the GDPR.

282. Article 26 GDPR reads as follows:

> *"1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.*
>
> *(...)"*

283. In the present proceedings, various entities from the Oracle and Salesforce groups have been summoned. In the case of group relationships, as discussed here, the legal person under whose authority the operational data processing occurs is in principle regarded as the controller. That does not affect the fact that together with other entities within the group, the purpose and

[204] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under 'How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform', consulted on 22 July 2020 (also **Exhibit 23.d**).
[205] See also CJEU 29 July 2019, case C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraph 66; CJEU 10 July 2018, C25/17, ECLI:EU:C:2018:551 (*Jehovan todistajat*), paragraph 66.
[206] Cf. CJEU 29 July 2019, case C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraph 80.

means for the data processing are established. As stated below in Section 4.5, all the parties summoned are involved in the processing in the context of the DMPs of Oracle and Salesforce. The various entities can therefore be considered as joint controllers within the meaning of Article 26(1) of the GDPR. Each of the controllers is liable for all of the data processing and compliance with the related obligations (Article 26(3) and Article 82(2) of the GDPR).

284. To the extent that Oracle and Salesforce should not be considered as the primary independent controllers, it holds that they are at least joint controllers, with their customers and/or other parties in the RTB ecosystem. In that case, the following applies:

a. Oracle and Salesforce are the joint controller with the Publishers as far as collecting personal data via cookies on Publishers' websites is concerned and for sharing personal data to the extent that it is directly related to the provision of advertising space on Publishers' websites (whether or not using an SSP);

b. Oracle and Salesforce are the joint controller with Advertisers for sharing data from the DMP with Advertisers (whether or not using a DSP);

c. Oracle and Salesforce are the joint controller for the exchange of data via cookie syncing with all parties with whom they exchange data in this way.

285. However, to the extent that Oracle and Salesforce were to hold the position that they are merely "processor", that position is untenable, given the above. It would also be contrary to the standpoint that there should be no lack of responsibility to ensure that data subjects are guaranteed effective and full protection.[207]

4.5 Territorial application

4.5.1 Territorial application of the GDPR

286. Article 3 of the GDPR governs the territorial scope of the GDPR:

> *"Article 3*
>
> *Territorial scope*
>
> *1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
>
> *2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> *a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

[207] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13. See also CJEU 05 June 2018, case C 210/16, ECLI: EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), paragraph 42.

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

[…]"

287. Under Article 3(1) GDPR, the GDPR applies to processing in the context of the activities of an establishment of a controller in the European Union ("**EU**").

288. Recital 22 illustrates this as follows:

> *"Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."*

289. Recital 19 of the Privacy Directive contained a similar text that has been cited several times by CJEU case law on the scope of that directive.[208] From that jurisprudence it can be derived that:

a. an "establishment" is "*any form of, even small, genuine and effective activity that is exercised through a fixed establishment*";[209]

b. there can already be a "*fixed establishment*" or "*stable arrangements*"[210] if there is one employee present in a country in the EU;[211]

c. the phrase "*in the context of the activities of an establishment*" should be interpreted broadly.[212]

290. When a predominantly non-EU enterprise has one or more establishments in the EU and the activities are "*inextricably linked*", the processing is deemed to take place within the context of the activities of that establishment (or those establishments) in the EU.[213] There is soon such a connection, for example, if a European establishment is dedicated to selling advertising space that enables the provision of a free search engine or social media platform.[214]

---

[208] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), CJEU 01 October 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*), CJEU 28 July 2016, C-191/15, ECLI:EU:C:2016:612 (*Amazon*) and CJEU 05 June 2018, C-210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie*); see also EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', version 2.1 ('EDPB Guidelines 3/20 Territorial Scope'), p. 6.
[209] CJEU 01 October 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*), paragraph 31.
[210] Recital 19 of the Privacy Directive speaks of "stable arrangements" and recital 22 of the GDPR also speaks of "stable arrangements", so both have "stable arrangements" in the English-language versions. It is thus in fact the same concept.
[211] CJEU 01 October 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*), paragraph 30.
[212] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), paragraph 53.
[213] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), paragraph 56 and EDPB Guidelines 3/20 Territorial Scope, p. 8-9.
[214] CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), paragraphs 56 and 57 and CJEU 05 June 2018, C-210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie*), paragraphs 58-60.

291. However, even if a controller does not fall within the scope of the GDPR through an establishment in the EU, pursuant to Article 3(2) GDPR, the GDPR is applicable in the case of processing data subjects in the EU in relation to the offering of goods or services or monitoring.

292. In the case of monitoring, the GDPR is only applicable in the case of monitoring the behaviour of a data subject that is located in the EU, while that behaviour also takes place in the EU.[215]

293. Recital 24 illustrates this as follows:

> *"The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."*

294. From this it is clear that the provision is in any case applicable to the monitoring of the behaviour of people on the Internet. Moreover, the EDPB thereby deems it relevant for which purposes the collected data are used and whether profiles are created and behavioural analysis takes place. The EDPB refers, inter alia, to "behavioural advertising" and "online tracking" by means of cookies as examples of monitoring activities that fall under Article 3(2)(b) GDPR.[216]

295. From Article 3(1) and Article 3(2)(b) of the GDPR, it follows that the GDPR applies to the processing of the personal data of Oracle and Salesforce.

296. The Oracle DMP service is offered primarily by the headquarters of the Oracle concern: Oracle Corporation in the United States. Oracle Corporation also appears to be the owner of the domain name that is used to place the bku cookies (bluekai.com).[217]

297. The role that Oracle Corporation plays in connection with the DMP service is confirmed in the privacy policy for Oracle Data Cloud, from which it may also be concluded that Oracle America, Inc. plays an important role in it too. This is because Oracle designates both Oracle Corporation and Oracle America, Inc. as controllers for the data processing:

> *"Oracle Corporation and Oracle America, Inc., with their registered address at 500 Oracle Parkway, Redwood Shores, CA, 94065, United States, are responsible for the processing of your personal data within the context of this Privacy Policy."*

[215] EDPB Guidelines 3/20 Territorial Scope, p. 19.
[216] EDPB Guidelines 3/20 Territorial Scope, p. 20.
[217] https://who.is/whois/bluekai.com, consulted on 22 July 2020.

298. Oracle also states that it is active in more than 80 countries and that the data is processed all over the world.[218] In the AddThis Privacy Policy (which is only available in English), the following is stated in respect of the controller for the data processing:

> *"Oracle Corporation and its affiliated entities are responsible for processing AddThis Data described in this Privacy Policy. A list of Oracle entities is available here. Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country."*

299. The list of Oracle entities for the Netherlands refers to Oracle Nederland B.V. Since AddThis is part of its DMP, with this information Oracle is also saying that Oracle Nederland B.V. too plays a role in the provision of the DMP service. Oracle's general privacy policy also contains a similar provision (in Dutch):

> *"Oracle Corporation and its affiliated entities are responsible for the processing of your personal information as described in this Privacy Policy. See the list of Oracle entities. To learn more, please go to the list of Oracle entities and select a region and country to see the registered address and contact details for the Oracle entity (entities) in each country."*

300. From the extract of the Chamber of Commerce (**Exhibit 26**), it appears that Oracle Nederland B.V. has 1,801 persons working for it and is active in such fields as the 'development, production and issuing of software' and in 'other service provision activities in the field of information technology'. Oracle Nederland B.V. is involved for instance in the sale and delivery of the products of the Oracle group in the Netherlands, including the DMP. This follows for instance from the fact that the 'Director Oracle Cloud Strategy - Northern Europe' is based in the Netherlands.

301. The Salesforce DMP service seems to be offered primarily by the headquarters of the Salesforce concern: Salesforce.com, Inc. in the United States. Salesforce.com, Inc. is also the owner of the domain name used for the placement of cookies (krxd.net).[219] Salesforce also provides the DMP service worldwide, including to customers in the Netherlands.

302. In the full privacy statement, Salesforce.com, Inc. and "the relevant affiliated companies" are regarded as controller "unless otherwise specified."[220] The list of affiliated companies includes, inter alia, "SFDC Netherlands BV".[221] In this way, Salesforce does not make it clear which entity is responsible for which processing operations.

303. From the extract of the Chamber of Commerce (**Exhibit 27**), it appears that SFDC Netherlands BV has 191 employees in the Netherlands and has activities in the field of "Providing services in the field of software applications to support organisations in managing customer data and documents." SFDC Netherlands BV is involved, inter alia, in the sale and delivery of products of the Salesforce concern in the Netherlands, including the DMP. This

[218] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under 9, consulted on 23 April 2020 (also **Exhibit 22.a**).
[219] Who.is, *krxd.net,* can be consulted via: https://who.is/whois/krxd.net.
[220] https://www.salesforce.com/nl/company/privacy/full_privacy/, under "1. Responsible Salesforce entity" and in the immediately preceding paragraph, consulted on 24 July 2020.
[221] https://www.salesforce.com/nl/company/locations/, consulted on 22 July 2020.

follows, inter alia, from the fact that the 'Senior Regional Vice President, Marketing Cloud' is located in the Netherlands.

304. Oracle Nederland BV and SFDC Netherlands BV are companies in the Netherlands. All processing operations within the context of their activities fall within the scope of the GDPR. This also includes the processing in the context of the DMP service, consisting of the collection, combination, enrichment, evaluation and selling of the personal data of Dutch Internet users. The GDPR is therefore applicable to this processing by Oracle Nederland BV and SFDC Netherlands BV.

305. Moreover, in the context of the above-mentioned jurisprudence, the companies are to be regarded as an "establishment" of the international companies Oracle and Salesforce respectively. Oracle Nederland BV and SFDC Netherlands BV are fixed establishments or stable arrangements. The entities are involved in, inter alia, the sale of the DMP service to publishers and advertisers in the Netherlands. These activities are inextricably linked with processing activities for which Oracle Corporation, Oracle America Inc. and Salesforce.com Inc., respectively, are (partly) responsible. Within the meaning of Article 3(1) GDPR, Oracle Nederland BV and SFDC Netherlands BV can therefore be regarded as an establishment of those foreign entities. The processing activities take place (partly) within the context of an establishment of the controllers in the EU. The GDPR is therefore also applicable to the processing activities for which Oracle Corporation, Oracle America Inc. and Salesforce.com Inc., respectively, are (partly) responsible.

306. Insofar as the processing activities of Oracle Corporation, Oracle America Inc. and Salesforce.com Inc., cannot be considered to take place within the context of the activities of an establishment in the EU, it holds that the GDPR is still applicable pursuant to Article 3(2)(b) of the GDPR. It is, after all, the processing of personal data of EU-based data subjects that is related to the monitoring of the behaviour of data subjects in the EU.

307. Oracle and Salesforce collect personal data by means of cookies that are placed, inter alia, on a large number of popular Dutch websites, at least websites that are frequented by Dutch people (**Exhibit 16**). In this way, Oracle and Salesforce follow the online behaviour of almost all Dutch Internet users. They are established in the Netherlands and the behaviour that is followed usually takes place in the Netherlands, and therefore within the EU. Oracle and Salesforce use the data to create profiles, and analyse and influence behaviour. There is online tracking by means of cookies and behavioural advertising.[222] There is cookie syncing for RTB. The processing activities of Oracle and Salesforce thus fall perfectly under Article(3)(2)(b) GDPR. Oracle Corporation, Oracle America Inc. and Salesforce.com Inc., respectively, are the parties that are ultimately responsible (within the Oracle and Salesforce groups) for providing the DMP services anywhere in the world and therefore also for the monitoring which that involves in the EU.

4.5.2 Territorial scope article 11.7a Tw

308. Article 11.7a Tw applies to "anyone" who stores or reads data on peripherals (such as a computer or a mobile phone) of an end user, regardless of where the party is located. In this

[222]Recital 24 of the GDPR and EDPB Guidelines 3/20 Territorial Scope, p. 20.

context, according to the ACM, a determining factor is that the standard is designed to protect end users in the Netherlands. That is why the information and consent requirement for the use of cookies applies to Dutch and foreign websites that (partly) focus on Dutch users. Whether websites focus on Dutch users can be derived, for example, from the nature of the information on the website, the possibility to deliver products in the Netherlands or the availability of the website in the Dutch language. The domain name extension (.nl / .eu / .com / .net / etc.) of the website is not decisive.[223]

309. Research (**Exhibit 16**) indicates that Oracle and Salesforce place cookies via numerous websites focused on the Netherlands. These are, for example, the website buienradar.nl, which provides updated information about rain in the Netherlands and by its nature is focused on the Netherlands. Both parties therefore place cookies on the peripherals of Dutch Internet users and read them out. Thus their behaviour is within the scope of article 11.7a TA, and they must ensure that they comply with the information and consent requirement.

4.6 Breach of the GDPR and Tw

310. The data processing of Oracle and Salesforce described in the factual framework is contrary to the fundamental right of respect for private life (Article 7 of the Charter) and the fundamental right to protection of personal data (Article 8 of the Charter), as developed, inter alia, in the GDPR and the Telecommunications Act. The following explains the relevant principles and provisions of the GDPR and Tw, and substantiates the breach.

311. Firstly, it is important that the actions undertaken by Oracle and Salesforce qualify as "profiling" within the meaning of Article 4(4) of the GDPR and, in view of the facts and circumstances, are prohibited under Article 22 of the GDPR. Secondly, Oracle and Salesforce do not have a valid basis for placing and reading cookies, in particular Oracle and Salesforce lack valid consent to perform these actions. Thirdly, Oracle and Salesforce do not meet the required transparency obligations about their actions, which take place largely out of the Internet user's sight. Fourthly, the gigantic collection of data is contrary to the principle of data minimisation. Fifthly, Oracle and Salesforce do not adhere to the principles of integrity and confidentiality and the way in which they are worked out in specific GDPR provisions. Sixthly, Oracle and Salesforce do not meet their accountability, which is also a core principle of the GDPR.

312. In the following, this very serious violation is further substantiated. The violation of fundamental rights by Oracle and Salesforce has already been discussed above. The following will first discuss the violation of the prohibition of profiling. The six violations referred to in the preceding paragraph shall then be explained. Finally, it will be shown that Oracle and Salesforce are also violating the GDPR in a variety of other ways.

4.6.1 Automated decision-making, including profiling

313. The factual framework explains that one of the main activities of Oracle and Salesforce is to create detailed profiles of Internet users. Oracle and Salesforce gather information from a variety of sources and give advertisers the tools to easily create "segments" or "audiences".

[223] *Parliamentary Papers I*, 2011/12, 32549, E, p. 7-8.

Oracle and Salesforce take advertisers by the hand and explain how they can make the audience more and more specific with just a few clicks of the mouse. The software of Oracle and Salesforce then links the attributes to the data it collects from different sources. The purpose of this data collection is to draw precise conclusions about the private lives of individuals. The data reveals many characteristics, such as daily habits, permanent or temporary residence, online reading behaviour and information about purchases.

314. In the case of profiling, the CJEU applies the relevant fundamental rights and the GDPR and Tw very strictly. The mere possibility of using data to create a profile leads to the conclusion that it concerns extremely sensitive information, which affects the core of the protection of fundamental rights that Articles 7 and 8 of the Charter protect. In the *Tele2* case, the CJEU puts it this way:

> *"That data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."* [224]

315. In the same way that a search engine such as Google plays a "decisive role" in making websites accessible by making them searchable based on certain characteristics, Oracle and Salesforce also play a decisive role in tracking and *targeting* Internet users online. After all, without Oracle and Salesforce, it is not possible to create the profiles, let alone the level of detail thereof.[225] While, according to the CJEU, Google's search results can only result in a "more or less detailed profile of the data subject"[226], the activities of Oracle and Salesforce lead to a very fine-grained profile of an identifiable person, a profile that is also increasingly refined in the context of RTB and the addition of additional information. The characteristics that can be mapped in this respect are sensitive or special categories of personal data, for example ethnicity, health and fitness, politics, religion and spirituality.

316. WG29 refers in its Profiling Guidelines to a study that combined simple Facebook "likes" with data from other sources. The researchers were able to determine the sexual orientation of male users in 88% of cases. In 95% of cases, ethnicity was well estimated. In 82%, the researchers made a correct prediction as to whether the Internet user was Christian or Muslim.[227]

317. The tools of Oracle and Salesforce make it possible to become more and more specific. "Digging a little deeper", Oracle calls it.[228] After creating an audience to which advertisements are shown using a variety of specific characteristics, Oracle and Salesforce show how large the audience is that is targeted by the advertisements.[229] Oracle and Salesforce tie all known information together and create a detailed profile that allows them to assess whether someone fits within

---

[224] CJEU 21 December 2016, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, (*Tele2*), paragraph 99.
[225] See CJEU 24 September 2019, C -136-17, ECLI:EU:C:2019:773 (*Google*), paragraph 36, describing Google as a party that plays a "decisive role" in making data accessible.
[226] See CJEU 24 September 2019, C/136-17, ECLI: EU:C:2019:773 (*Google*), paragraph 36.
[227] Article 29 working party, Guidelines concerning automated individual decision-making and profiling for the application of Regulation (EU) 2016/679, as most recently amended and established on 6 February 2018, WP251rev.01, p. 18 ('WP251 Profiling').
[228] Oracle Create Audience Segments, **Exhibit 13**, also available via: https://learn.oracle.com/ords/launchpad/learn?page=create-audience-segments&context=0:41799:41822, consulted on 22 July 2020.
[229] Salesforce Segment Builder Guide, **Exhibit 14**, also available on https://konsole.zendesk.com/hc/en-us/articles/217950467-Segment-Builder-Guide, consulted on 22 July 2020.

an audience. They can also specify audiences using the profiles of people who fall within the target group. Thanks to cookie syncing, as described above, the profiles become even more specific.

318. This creates a fine-grained web of profiles, where every Internet user is pigeonholed based on their supposed preferences and interests. In its Guidelines, WG29 identifies various risks of profiling, including undermining the freedom of choice for certain products or services.

> *"Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination."* [230]

319. Article 4(4) of the GDPR defines "profiling" as follows:

> *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"*

320. This is exactly the activity that Oracle and Salesforce perform. After all, it is a form of *automated* processing. The services of Oracle and Salesforce are typical examples of big data applications. Millions of data are collected daily through cookies, enriched with other sources and linked to other cookie identifiers, which are analysed automatically in order to recognise correlations. As WG29 points out in its Guidelines, a certain degree of automated processing is sufficient; human intervention does not mean that the activity does not fall within the definition.[231] Moreover, the data processing of Oracle and Salesforce also concerns personal data (the second requirement). Thirdly, it aims to evaluate the personal aspects of a natural person.

4.6.1.1 Prohibition of exclusively automated decision-making

321. The activities of Oracle and Salesforce are contrary to Article 22 of the GDPR. The GDPR contains specific new provisions for combating the risks arising from profiling and automated decision-making. With Article 22(1) of the GDPR, the European Legislator introduced no less than a prohibition to take decisions based solely on the automated processing of personal data, if those decisions have legal effects or if they otherwise affect the data subject to a significant extent.[232] Article 22(1) of the GDPR reads as follows:

[230] WP251 Profiling, p. 6.
[231] WP251 Profiling, 7.
[232] Although the text of Article 22(1) has been formulated as a right ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."), this is not a right that should be invoked, but a prohibition. See also WP251 Profiling, p. 23: "The term "right" in this provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data."

> *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*

322. For example, a decision with legal effect is the termination of an agreement or the refusal of a licence. Article 22(1) of the GDPR is not however limited to decisions having a legal effect. In its Guidelines, WG29 states explicitly that online advertising, when using automated tools, can affect the data subject to a considerable extent and thus may fall under the prohibition. As described, placing cookies, cookie syncing and the RTB process is eminently a purely automated process that takes place in a few seconds, and that, given the speed, the amount of data and the number of players, can take place in no other way than solely automated. The same applies to the way in which data is enriched by the DMPs.

323. WG29 names as factors relevant to assessing whether online advertising is covered by the prohibition:

> *"• the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;*
>
> *• the expectations and wishes of the individuals concerned;*
>
> *• the way the advert is delivered; or*
>
> *• using knowledge of the vulnerabilities of the data subjects targeted.*[233]

324. These are outstanding features of the practice of Oracle and Salesforce as described above. After all, inter alia, by means of cookie syncing, there is a large-scale and intrusive profiling process in which personal data are collected by different websites, devices and services. The individuals concerned are not at all aware of the scale, the number of players involved in the background and the level of detail of the profiling. Precisely because of the fine-grained profile, the data subject can be very specifically *targeted* and can be shown the most relevant advertisements, making full use of the knowledge about vulnerabilities of data subjects.

325. Inherent to the level of detail of the profiling, *digging a little deeper*, and the scale and efficiency of the automated process of the DMPs is that use will be made of the vulnerabilities of data subjects. WG29 emphasises this in the Guidelines on profiling:

> *"Processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults. For example, someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt."*[234]

326. In Article 22(2) of the GDPR, three exceptions are made to the prohibition of automated decision-making, including profiling. Oracle and Salesforce cannot invoke any of these exceptions.

---

[233] WP251 Profiling, p. 26.
[234] WP251 Profiling, p. 26.

327. It must be stated firstly that, according to the established case law of the CJEU, exceptions to the GDPR must be interpreted strictly, because they put aside the protection provided for in the Regulation and thus derogate from the purpose intended by the GDPR, the protection of fundamental rights.[235]

328. The first exception is applicable when the controller is able to demonstrate that profiling is necessary in order to enter into or execute the agreement, for example, a subscription to a streaming service, which makes as specific as possible suggestions matching the interests of the subscriber on the basis of a profile. Now that there is no question of an agreement between Oracle and Salesforce on the one hand and the data subject on the other, this exception does not apply.

329. The second exception is applicable when automated decision-making and profiling is explicitly authorised by Union law or Member State law that is applicable to the controller. An example is a law that allows automated decision-making to detect tax fraud. There is no question of such a legal exception in the practices of Oracle and Salesforce.

330. The commercial interests of major players in the *AdTech* market to create intrusive digital profiles of European data subjects and the widespread international exchange thereof is not an interest that the legislator will want to recognise with a legal exception. On the contrary, precisely with the GDPR, the European Legislator has wanted to introduce a strong and coherent legal framework, backed by strict enforcement, in order to give data subjects a consistent and high level of protection in times of rapid technological change and globalisation.

331. The third exception applies when the data subject has given *explicit* consent for the automated decision-making and profiling. As will be described below, there is no valid consent, let alone explicit consent specifically with regard to the automated decision-making and profiling.

332. To the extent that the first (agreement) or third (explicit consent) is already eligible, these exceptions can only be used if the controller has taken appropriate measures to protect the data subject. In any case, specific information should be provided to the data subject about the processing (recital 71 GDPR). Furthermore, the data subject should have the opportunity to involve someone ("right to human intervention"), to make his or her position known, to obtain an explanation of the decision thus taken and to challenge the decision. Insofar as Oracle and Salesforce could even be successful in invoking one of the above exceptions, then, for example, the specific information requirement is not even met, as will be explained below.

333. As is already evident from the passage of the WG29 cited above about Facebook-likes, it is, moreover, almost inherent to large-scale and fine-grain profiling that sensitive personal data will be processed, to the extent that this is not already done deliberately. By linking information from different sources, it is possible to make such accurate predictions about, for example, sexual or religious preferences or health, that intensive active operations will be required so as *not* to process sensitive personal data.

[235] CJEU 14 February 2019, C -345/17, ECLI:EU:C:2019:122, (*Buivids*), paragraph 41 and the case law cited there.

334. Insofar as Oracle and Salesforce can already use the exceptions to the prohibition on automated decision-making and profiling, it holds that no use may be made of special data, unless there is the explicit consent of the data subject (Article 9(2)(a) GDPR) or there is a substantial public interest (Article 9(2)(g) GDPR). Oracle and Salesforce do not meet these conditions. In both cases, the controller must, moreover, take appropriate measures to safeguard the rights, freedoms and legitimate interests of the data subject.

335. Although Article 22 itself makes no distinction between adults and children, recital 71 states that solely automated decision-making, including profiling, which produces legal effects or otherwise significantly affects the data subject, may not apply to children. In its Guidelines, WG29 explains that this should be so interpreted that in principle, controllers may not use the exemptions of Article 22(2) to justify this type of processing.[236] Incidentally, here WG29 adds to this that organisations *in general* should refrain from the profiling of children for marketing purposes.[237]

4.6.1.2 Other specific requirements for profiling

336. The GDPR focuses not only on the decisions taken on the basis of automated processing or profiling, but is applicable to the collection of data to create profiles and the application of these profiles to people. Outside the scope of the exceptions to the prohibition on automated decision-making, the legislator also refers in several places explicitly to additional appropriate safeguards that are to be taken in the context of profiling in general.

337. For example, there are specific requirements relating to transparency, as is also described in recital 60:

> *"Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling."*

338. This is supplemented in recital 63:

> *"Every data subject should therefore have the right to know and obtain communication in particular with regard to [...] the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing."*

339. Data subjects also have the right to object to profiling and specifically profiling for marketing purposes, as is also described in recital 70:

> *"Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information."*

[236] WP251 Profiling, p. 34.
[237] WP251 Profiling, p. 35.

340. Incidentally, in the context of profiling, stricter obligations apply in relation to accountability (for example, pursuant to Article 37(1)(b) of the GDPR), and, if certain conditions are met, there is the requirement to execute a data protection impact assessment (Article (35)(3)(a) GDPR).

4.6.1.3 Conclusion with regard to automated decision-making and profiling

341. Given the above, Oracle and Salesforce act contrary to Article 22 of the GDPR. To the extent that your Court were to consider that, in spite of the above, Oracle and Salesforce act in accordance with Article 22, that by no means implies that the practice of Oracle and Salesforce is permitted. The fact that there is profiling within the meaning of Article 4(4) GDPR implies that the other conditions of the GDPR will have to be assessed with additional strictness. It will be explained below that in any event, Oracle and Salesforce do not satisfy, inter alia, the principles of lawfulness, transparency and data minimisation.

4.6.2 Lawfulness – unlawful processing, no valid consent

4.6.2.1 Consent is the only basis that qualifies

342. Processing of personal data should always be based on one of the six limiting principles of Article 6 GDPR.[238] If none of these principles apply, the processing is unlawful. For the processing to which this case relates, only the principles of "consent" (a) and "legitimate interest" (f) are eligible for consideration.

343. Article 6 GDPR reads, insofar as is relevant:

> *"Lawfulness of processing*
>
> *1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
>
> *[…]*
>
> *f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*
>
> *[…]"*

344. Oracle acknowledges that the data processing it carries out can only be legitimised on the basis of "consent". Oracle explicitly states this in its Oracle Data Cloud Privacy Policy:

> *"We rely on your consent for the purpose of enabling Oracle Marketing & Data Cloud customers and partners to market products and services to you, including*

[238] Dutch Data Protection Authority, "Interpretation of the basis of 'legitimate interest'", 01 November 2019, p. 1.

> *measurement and analytics on campaign performance, personalization, modelling, onboarding, and linkage (see Section 5 above for additional details on these purposes). Your consent is obtained on behalf of Oracle and its Oracle Marketing & Data Cloud customers and partners by our third party data providers* (…)"[239]

345. Oracle, however, is of the opinion that it is not responsible for obtaining this consent. It is of the opinion that Oracle's partners should ask for consent on behalf of Oracle.

346. It is not or not sufficiently clear from the privacy documentation of Salesforce on what basis it bases its data processing. In its "Trust and Compliance Documentation", Salesforce indicates that its partners are responsible for asking consent, at least, to the extent that it is legally required:

> *"The Audience Studio Services enable customers to use cookies and/or other tracking technologies. Customers shall be solely responsible (i) for assessing whether such technologies can be used in compliance with applicable legal requirements, and (ii) for providing notice and/or obtaining consent, as may be required by law, for such use of cookies and/or other tracking technologies. Salesforce disclaims any liability to customers or any third parties arising from customers' use of any cookies and tracking technologies." (**Exhibit 23.f**)*

347. This "Trust and Compliance Documentation" is moreover aimed at (potential) customers of Salesforce and is extremely difficult to find for a Dutch Internet user (see also Section 4.3.1.2). From this it is, however, evident that Salesforce does not exclude that consent must be asked. Salesforce also leaves the asking of consent to its customers. It is unclear on what basis its data partners collect, process and provide personal data to Salesforce.

348. Note that once a choice has been made for a basis, this cannot be changed later.[240] Oracle and Salesforce are not therefore (any longer) allowed to submit an additional or alternative basis (such as legitimate interest); at least if they were to do so, it would again constitute a breach of the GDPR.

349. The crucial role of consent is emphasised in Article 8 of the Charter, as is also confirmed by the WG29 and EDPB.[241]

350. In the following, it will be explained that "consent" in this case is the only valid basis for the data processing, that Oracle and Salesforce cannot delegate the obtaining of consent to their customers and that the consent, whether or not obtained via these customers, does not meet the criteria of legal consent.

---

[239] Oracle Data Cloud Privacy Policy, under 6 "For information about you collected in the EU/EEA, what is our legal basis?", see https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, accessed on 14 July 2020, (also **Exhibit 22.a**).

[240] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, ('EDPB Guidelines 05/2020 Consent') 04 May 2020, p. 25 par. 120; Working Party Article 29, Opinion 15/11 on the definition of consent, 13 July 2011, WP187, p. 8 ('WP187 Definition of consent'), p. 21.

[241] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, ('EDPB Guidelines 05/2020 Consent') 04 May 2020; Working Party Article 29, Opinion 15/11 on the definition of consent, 13 July 2011, WP187, p. 8 ('WP187 Definition of consent').

Claiming legitimate interest not possible

351. It must be stated firstly that the basis of Article 6(f) GDPR is not eligible. First of all, with regard to placing and reading cookies, article 11.7a Tw stipulates that consent is the only possible basis. [242] Moreover, this also follows from the judgment of the CJEU in the *FashionID* case, concerning the installation of a social plug-in, a technique similar to cookies to which Article 5(3) of the e-Privacy Directive (article 11.7a Tw) applies:

> *"87. By its fourth question, the referring court asks, in essence, whether, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plug-in causing the browser of a visitor to that website to request content from the provider of that plug-in and, to that end, to transmit to that provider personal data of the visitor, it is appropriate, for the purposes of the application of Article 7(f) of Directive 95/46, to take into consideration a legitimate interest pursued by that operator or a legitimate interest pursued by that provider.*
>
> *88. As a preliminary point, it should be noted that, according to the Commission, this question is irrelevant for the resolution of the dispute in the main proceedings, since consent was not obtained from the data subjects as is required by Article 5(3) of Directive 2002/58.*
>
> *89. In that regard, it should be pointed out that Article 5(3) of Directive 2002/58 provides that Member States are to ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is allowed only on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46, inter alia, about the purposes of the processing."* [243]

352. Insofar as Oracle and Salesforce would nevertheless invoke the basis of legitimate interest, it holds that this does not apply either, because:

a. There is no question of legitimate interest, namely merely a purely commercial interest;

b. The processing is not necessary, because it is not proportional;

c. The interests, rights and fundamental freedoms of data subjects outweigh the purely commercial interests of Oracle and Salesforce.[244]

4.6.2.2 It is not possible to delegate the obtaining of consent

353. Oracle and Salesforce cannot delegate the obtaining of consent to their customers for at least three reasons.

354. Firstly, it holds that it is not the customers of Oracle and Salesforce who place cookies, but Oracle and Salesforce themselves (see under Section 3.2.1). That is evident, inter alia, from the

[242] See article 11.7a TA(3).
[243] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 (*Fashion ID*).
[244] Cf. Dutch Data Protection Authority, Interpretation of the basis of 'legitimate interest', 01 November 2019.

fact that the cookies bear the names that Oracle and Salesforce have assigned them, and are technically associated with the domain of Oracle and Salesforce. The data transmission takes place between the peripheral equipment of the Internet user and the servers of Oracle and Salesforce. It is also Oracle and Salesforce that are responsible (for the processing) here. This also applies to the operations which they perform subsequent to placing the cookie and the resulting collection of information, namely profiling, enriching profiles with information from other sources, offering profiles in the context of real-time bidding and cookie syncing.

355. Secondly, it holds that the customers of Oracle and Salesforce cannot ask for legal consent for these activities because they are not (fully) aware of these activities. The customers of Oracle and Salesforce, for example, are not aware of the manner in which a DMP exchanges unique identifiers of cookies with other partners in the *AdTech* industry and how the information thus obtained is tied together by means of cookie syncing.

356. Thirdly, these customers cannot possibly obtain legal consent because they can never fully and specifically inform Internet users about the scope of the data processing. At every auction in the context of RTB, data are shared with hundreds of parties. Oracle and Salesforce share data with such a large, diverse group that it cannot even be known at the start of an auction. It is actually impossible for such an extensive processing, through a multiplicity of parties, to provide adequate information on, inter alia, the identity of those parties. It is also impossible to adequately inform about all the purposes of the processing of all those parties.

357. To the extent that your Court were to consider that Salesforce and/or Oracle can delegate the obtaining of consent in this case to their customers and/or partners, it holds that any consent obtained by them does not meet the conditions imposed thereon by the GDPR and Tw. The burden of proof that legal consent has been obtained rests on Oracle and Salesforce (inter alia Article 7(1) GDPR).

4.6.2.3 <u>There is no question of valid consent</u>

358. Article 4(11) GDPR defines "consent" as follows (Lawyer's underlining):

> *"any <u>freely given</u>, <u>specific</u>, <u>informed</u> and <u>unambiguous indication of the data subject's wishes</u> by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"*

359. That means that consent only yields a valid basis under Article 6 GDPR when it is (i) freely given, (ii) specific, (iii) informed and (iv) unambiguous. Consent under article 11.7a Tw must meet the same conditions as consent under GDPR Article 6. This is also evident from the judgment of the CJEU in the *Planet49* case [245] and from the wording of article 11.7a Tw.

360. The processing of personal data by Oracle and Salesforce does not meet these conditions.

<u>(i) Freely given</u>

361. First, there is no question of freely given consent. Freely given consent means that the data subject can make a real choice. If the data subject feels more or less compelled, or if it has negative consequences for him if he withholds or withdraws his consent, then there is no

[245] CJEU 01 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).

question of valid consent. It is the responsibility of the controller to demonstrate that the data subject actually had a free choice, and that it was possible not to give consent or to withdraw the consent without detriment (recital 42 GDPR). [246]

362. In connection with the requirement that consent must be freely given, it is not allowed to require consent as (indirect) compensation in return for providing a performance (including a service). If the processing is not necessary for providing the performance, delivering that performance should not be conditional on obtaining the personal data on the basis of consent (Article 6(4) and recital 43 of the GDPR).[247]

363. Remarkably, a large proportion of websites do not ask for any consent at all before cookies are placed. The technical research shows that at least 22 of the 100 websites investigated place cookies before or without asking for consent, of which cookies were placed on 12 Salesforce websites and on 10 Oracle websites (**Exhibit 16**).

364. Other websites set consent for the use of cookies as a condition for visiting the website, this is also known as a "cookie wall". From **Exhibit 18** it is evident that no less than nine of the websites through which Oracle and Salesforce place their cookies, and that are (also) focused on Dutch Internet users, make use of a cookie wall. This consent is not freely given. After all, for the data subject it is not possible to withhold consent without experiencing detriment.[248] Delivering the service, access to the website, is thus made dependent on the giving of consent, while the processing is not necessary for the provision of the service.[249] From the judgment of the CJEU in the *Planet49* case, it follows that asking for consent in such a way, which does not require any active action, is not permitted.[250]

365. The Data Protection Authority is also very clear that valid consent cannot be obtained with a cookie wall:

> *"May I, as an organisation, use a cookie wall?*
>
> *With a cookie wall, website visitors have no real or free choice. Although they may reject tracking cookies, that cannot be done without adverse consequences. Because rejecting tracking cookies means that they are unable to access the website. Therefore cookie walls are prohibited under the GDPR."*[251]

366. Secondly, there is no question of freely given consent if the consent to different processing operations or purposes is interconnected. When a service includes multiple processing operations or purposes, the data subject should be able to choose freely for which processing and/or purposes he gives consent, and which not. If a data subject can only give consent for a

[246] EDPB Guidelines 05/2020 Consent, p. 13.
[247] See further the EDPB Guidelines 05/2020 Consent, p. 10-12.
[248] Cf. EDPB Guidelines 05/2020 Consent, p.10.
[249] Cf. EDPB Guidelines 05/2020 Consent, p. 10-12.
[250] CJEU 01 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[251] Data Protection Authority, 'Cookies', can be consulted via: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies; Cf. also EDPB Guidelines 05/2020 Consent, p. 12 par. 39.

package of processing operations and/or purposes, the consent is not considered to be freely given (recitals 32 and 43 of the GDPR).[252] Or as the WG29 formulates it:

> *"If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom."*[253]

367. The latter sub-requirement is also called "granularity" and is related to the requirement that consent must be specific (see below). That requirement is not satisfied by Oracle and Salesforce. The data subject must, after all, almost always give consent for a whole range of tracking cookies of different parties for different processing operations and for different purposes (see marginal 389). Oracle and Salesforce do not therefore obtain freely given consent.

368. That the consent is not freely given is also evident from the many public surveys that have been done on the use of tracking technologies. Only 20% of Europeans agree with the sharing of data with third parties for advertising purposes.[254] 37% use software to guard against tracking technologies. A recent study, where users were offered a website where visitors actively had to click on an opt-in for the use of tracking technologies, resulted in 0.1% of users who gave the opt-in.[255]

(ii) Specific

369. The requirement that consent must be specific means that it must be clear to the data subject for what he exactly gives consent. The requirement is intended to ensure transparency and control for data subjects.

370. In this context, it should be clear for what purposes the controller asks consent. Moreover, in addition the need for granularity again applies: the data subject must be able to choose for each processing operation and purpose whether he gives consent or not. General consent for processing operations "for advertising purposes" does not satisfy this. Along with the principle of purpose limitation (Article 5(1)(b) GDPR), the requirement that consent must be specific serves as protection against the gradual expansion of processing (also known as "function creep").[256]

371. The consent must also be sufficiently specific about the data being processed.[257] In general, the consent must be specific such that the data subject knows exactly for what he gives consent:

> *"It should be added that the indication of the data subject's wishes referred to in Article 2(h) of Directive 95/46 must, inter alia, be 'specific' in the sense that it must*

[252] EDPB Guidelines 05/2020 Consent, p.12 par. 42-44.
[253] Working Party Article 29, Guidelines for consent under Regulation 2016/679, WP259 rev. 01, as recently amended and adopted on 10 April 2018 and as endorsed by the EDPB on 25 May 2018, ('WP259 Guidelines for consent under Regulation 2016/679') 11; an almost identical text is still included in the latest version of these guidelines, which are only available in English, see EDPB Guidelines 05/2020 Consent, p. 12 par. 44.
[254] GfK, "Europe Online: an Experience Driven by Advertising. Summary results", September 2017, p. 7, can be consulted via: https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf
[255] C. Utz, et.al. '(Un)informed Consent: Studying GDPR Consent Notices in the Field', 22 October 2019, accessed on 04 May 2020, on: https://arxiv.org/pdf/1909.02638.pdf.
[256] EDPB Guidelines 05/2020 Consent, p. 14 and 15.
[257] EDPB Guidelines 05/2020 Consent, p. 15 par. 61.

relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes." [258]

372. The consent to the processing of personal data by Oracle and Salesforce is not specific. It is absolutely unclear to the data subject to what exactly he gives consent if he clicks on "Consent" or "Accept cookies" on the website of a partner of Oracle and Salesforce. Oracle and Salesforce ask consent for various processing operations and purposes (collecting, enrichment, sharing, analysing and selling) all at once. Thus they do not make clear exactly what data is being processed.

(iii) Informed

373. The consent obtained by (the customers and/or partners of) Oracle and Salesforce is not "informed" either.

374. The provision of information to data subjects before they give consent is necessary to enable them to make an informed decision and to understand what they agree to. This is necessary to enable the data subject to exert control over what happens to their data. There is a high standard for the clarity and accessibility of the information to be provided. If consent is sought, it must be in clear and straightforward language, that is comprehensible to the average person. Information that is relevant to making an informed decision about whether or not to give consent may not be hidden in general terms and conditions.[259]

375. According to the WG29, to give informed consent, the following information must in any case be provided:

a. The identity of the controller;

b. The purposes of the processing operation for which consent is asked;

c. What (type of) data are processed;

d. The right to withdraw consent;

e. Information about automated decision-making; and

f. Information on transfer of personal data outside the EU.[260]

376. If there are several (joint) controllers that claim consent, they will all have to be named.[261] The controller must ensure that consent is granted only on the basis of information that enables the data subject to easily establish who is the controller or who are the (joint) controllers.[262]

377. In the *Planet49* case, the CJEU has also emphasised the need to provide information about the duration that cookies are active and whether or not third parties have access to the cookies:

[258] CJEU 01 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*); see also X.
[259] EDPB Guidelines 05/2020 Consent, p. 16 par. 67.
[260] EDPB Guidelines 05/2020 Consent, p. 15.
[261] EDPB Guidelines 05/2020 Consent, p. 16.
[262] EDPB Guidelines 05/2020 Consent, p. 16.

> *"By Question 2, the referring court asks, in essence, whether Article 5(3) of Directive 2002/58 must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies."* [263]

378. Now that the activities of Oracle and Salesforce should be classified as "profiling", there is a greater obligation to clear communication, so that the data subject understands exactly for what he gives consent, as is also emphasized by WG29:

> *"Profiling can be opaque. Often it relies upon data that is derived or inferred from other data, rather than data directly provided by the data subject. Controllers seeking to rely upon consent as a legal basis for profiling will need to show that data subjects understand exactly what they are consenting to, and remember that consent is not always an appropriate basis for the processing. In all cases, data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice."*[264]

379. Oracle and Salesforce have sought to partly delegate the information to the customers and/or partners that provide the websites on which the cookies are placed. As far as possible, the burden of proof that legal consent has been granted rests, as stated earlier, with Oracle and Salesforce pursuant to Article 7(1). Without thereby suggesting that the burden of proof of this (also) rests on the Foundation, it notes that it follows from its research that a large proportion of the websites of its customers and/or partners contain no or hardly any information.

380. **Exhibit 18** shows a list of 41 websites which, according to the research of Dr. Bashir (**Exhibit 16**), make use of Oracle and/or Salesforce cookies. It follows from this that at least 16 websites make no mention whatsoever of the use of cookies or services of Oracle and/or [Salesforce]. Another four websites place no link to the privacy documentation of Oracle and/or Salesforce, and another 11 websites do have a link, but to the wrong document. Through 31 of the 41 websites, it is therefore not possible at all to arrive at the relevant information of Oracle and Salesforce. **Exhibit 28** includes a number of examples of how the parties point to the use of cookies on their website.

381. When information *is* provided by the customers and/or partners of Oracle and Salesforce, that occurs mostly in different layers. In the most favourable structure that looks like this:

a. The first information layer is a so-called *cookie banner* that appears when the data subject visits a website for the first time. A cookie banner is usually a bar at the top or bottom of the page, which the visitor can choose to close or leave in place. The bar only contains limited information, such as that the website uses cookies for advertising purposes. Further, the bar often contains a link that refers to more information about cookies.

[263] CJEU 01 October 2019, C-673/17, ECLI: EU:C:2019:801 (*Planet49*), paragraph 72 to 81.
[264] Working Party Article 29, Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EC) 2016/679, 03 October 2017, as recently amended and adopted on 06 February 2018, WP251, rev.01 ('WP251 Profiling'), p. 14 and 15.

b. When the data subject clicks on the link in the cookie banner (often called "More information" or "Cookie policy"), he is redirected to a document which is supposed to (also) give information about the cookies that are placed via the customer's and/or partner's website ("**Partner Cookie Policy**").

c. In the optimal scenario, the Partner Cookie Policy contains information about all cookies, such as functional, analytical and ad cookies, which can be placed via the website, including those of Oracle and Salesforce, including a link to relevant information of Oracle and Salesforce. So the customers and/or partners delegate the provision of information, in turn, to Oracle and Salesforce. Simply referring in this way to the documentation of Oracle and Salesforce as well as to numerous other parties does not in itself satisfy the requirement that consent must be "informed".

382. That there is a question of acting in breach of this requirement, is the more evident now that the documentation of Oracle and Salesforce only includes some scattered information regarding their cookies.

383. Oracle does not indicate at all for which specific processing operations it places and uses cookies for marketing purposes. Oracle only states that cookies are used:

> "to recognize you and/or your device(s) on, off and across different services and devices for the purposes specified in Section 5 above."
>
> And:
>
> "We or our Oracle Marketing & Data Cloud partners may use cookies to, among other things, track user trends and collect information about how you use our customers' sites or interact with advertising."[265]

384. Information about the cookie name, cookie life and who placed the cookie is missing.

385. Salesforce merely states that Cookies are used and that they contain a "unique, pseudonymized Audience Studio user ID" (Essentially a Cookie ID). It does not state what is done with these cookies.[266] There is also no information about the cookie name and who placed the cookie. Salesforce does mention the lifetime of the cookie.

386. Both sides mention nothing about linking Cookie IDs with other parties in the context of cookie syncing, as described in the factual part above.

387. It is clear that even in the most favourable scenario, this type of information provision does not at all make clear to the data subject what to expect. The data subject will have to struggle through an endless list of technical cookie information from a variety of parties and will have to continue to click through to the information of the third parties involved. In this way it cannot become clear exactly what information is collected by which parties and for what they

[265] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, "12. What cookies, pixel tags and other similar technologies do we use?", accessed on 24 July 2020.
[266] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under "HTTP Cookies", consulted on 27 July 2020 (also **Exhibit 23.d**).

use it. The way the information is made available does not satisfy, inter alia, the accessibility requirement.[267]

388. In addition, the information does not contain all required elements. For example, the data subject is unable to determine who are the (joint) controllers and for what purposes they use the data exactly.[268]

389. It is also evident from **Exhibit 18** that only 7 of the 41 websites investigated offer the opportunity to give consent per AdTech party. For the other 34 websites it is all or nothing. At many sites, this also means that exchanges of personal data with alarming numbers of AdTech partners are allowed. For example RTL, the manager of RTL Nieuws, Buienradar and Videoland, admits sharing data with 250 AdTech partners.

390. It is also striking that even after considering all possible relevant documentation, including cookie policies of the partners and the available privacy documentation of Oracle and Salesforce, it remains unclear how exactly the personal data in the RTB ecosystem are collected, enriched, combined and shared. Consequently, it will be unclear to the data subjects what the consequences of the processing (which also comprises profiling) can be.

391. When looking specifically at the information that Oracle and Salesforce themselves make available, it appears that this is difficult to understand and incomplete (**Exhibit 22 and Exhibit 23**). A portion of the Salesforce information is moreover unavailable in its entirety on the Dutch website and very hard to find for Dutch Internet users (see Section 4.3.1.2). Even if the data subjects were to get the information, which is unlikely, it is still incomprehensible what the consequence is of giving consent.

392. In the information on Oracle's website, many aspects of Oracle's processing operations remain unspecified. It is still unclear that Oracle monitors not only online but also offline behaviour, and how it enriches data with large amounts of information from multiple sources. Thus it does not make clear, inter alia, what (type of) data it processes.

393. For the Salesforce website, it holds that Dutch visitors are automatically directed to the Dutch page of the website. As described above, that includes hardly any information about the DMP service of Salesforce. Only the English version has some specific information available on this service. From this too, it is not evident what information exactly Salesforce collects, from what sources, with whom it shares the data and for what purpose the data are used.

394. Given the foregoing, this does not meet the requirement of informed consent.

(iv) Unambiguous indication of the data subject's wishes

395. Fourthly, it is required that consent is given by means of an unambiguous indication of the data subject's wishes. It should be a statement by the data subject or some other clear affirmative action proving that the data subject wishes to give its consent to a specific processing. This action must be intentional. Pre-ticked opt-in boxes are unlawful, and also

[267] EDPB Guidelines 05/2020 Consent, p. 16.
[268] EDPB Guidelines 05/2020 Consent, p. 16 par. 68.

silence, inactivity or continuing to use a service or website are insufficient.[269] After all, in such cases it cannot be excluded that the data subject has not even noticed or read the information.[270]

396. In the *Planet49* case, the CJEU emphasised that a for free, specific, informed and unambiguous expression of will, in any event a "clear affirmative action" is required. A website that uses pre-ticked opt-in boxes does not satisfy this.

> *"62. Active consent is thus now expressly laid down in Regulation 2016/679. It should be noted in that regard that, according to recital 32 thereof, giving consent could include ticking a box when visiting a website. On the other hand, that recital expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent."*[271]

397. The same applies to websites that use a "cookie wall", deriving consent from continuing to visit a website or only offering the opportunity to raise objections. Such consent does not meet the criterion of an unambiguous indication of the data subject's wishes, because there is no active or deliberate action.[272]

398. **Exhibit 18** shows a list of websites which, according to the research of Dr. Bashir (**Exhibit 16**), make use of Oracle and/or Salesforce cookies. The list shows that many of the websites do not ask for consent in the correct way and/or fail to provide information on the processing of personal data by Oracle and Salesforce. Of the 41 websites, 16 websites place cookies as soon as the Internet user visits the website, that is, before being given consent. Nine websites use a cookie wall, 32 use a banner. Of the websites that use a banner, nine derive consent from continuing to visit the website without providing the opportunity to refuse cookies. In addition to this, only two websites provide the opportunity to refuse tracking cookies just as easily as to allow them, namely with one click in the cookie banner. On all other websites that provide at least some opportunity to refuse cookies, the Internet user must click several times.

399. Even if the data subject actually has to click on "Agree" or "Consent", it cannot be said that he actually expresses his intention for a specific processing based on a full and specific warning of the consequences of giving consent. As described above, the data subject must make his way through different layers of information and various documents from many different parties (to the extent that such documentation is actually provided). Oracle and Salesforce have thus structured the information that a data subject is essentially unable to indicate unambiguously to what he agrees. Clicking "Agree" or "Consent" in relation to RTB essentially indicates no more than that the data subject expresses his wish to continue browsing.

<u>Other requirements for valid consent</u>

400. The GDPR provides a number of additional requirements for consent.

---

[269] EDPB Guidelines 05/2020 Consent, p. 18 par. 79; see recital 32 of the GDPR and also CJEU 01 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*), paragraphs 44 to 64.
[270] CJEU 01 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*), paragraph 55.
[271] CJEU 01 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[272] EDPB Guidelines 05/2020 Consent, p. 18.

401. Firstly, the controller has the duty to prove that the data subject has given consent (Article 7(1) and recital 42 of the GDPR). In addition, the controller also has to be able to demonstrate that the data subject has been informed and that the workflow for obtaining consent met all the above requirements.[273] The controller will have to be able to demonstrate, inter alia, what information has been provided, in what manner, and how the data subject has expressed his wishes.

402. Secondly, the GDPR sets the requirement for consent that the data subject should always be able to withdraw consent (Article 7(3) GDPR). In addition, the withdrawal of consent should be as simple as giving it (also Article 7(3) GDPR). Thus, when consent is obtained by means of a single click of the mouse, the data subject must also be able to withdraw consent with a single click of the mouse, or, in any case, just as easily.[274]

403. After withdrawal of consent, the controller will have to stop all data processing based on consent. Personal data must be erased, unless they are also processed for another purpose with another legal basis. That legal basis must in that case already have been in place when the processing began, and in this context it is also important that it has been clear and transparent from the outset what data are processed for what purposes and the legal basis that is invoked. After the consent is withdrawn or proves to be invalid, the controller cannot change to a different legal basis.[275]

404. The easy withdrawal of consent is a necessary aspect of valid consent. Now that Oracle and Salesforce do not offer this possibility, there is no question of valid consent.

405. Finally, even if the controller invokes the basis of consent, the controller has the duty to achieve a balance of interests, taking into account the principles of proportionality and subsidiarity. The principle of proportionality implies that the infringement of the interests of the data subject may not be disproportionate to the purpose of the processing. On the basis of the principle of subsidiarity, it is a requirement that the purpose cannot be achieved in another manner, which would be less detrimental to the data subject. In making the consideration, all the circumstances of the case must be taken into account.[276]

406. In the present case, it holds that Oracle and Salesforce collect large volumes of data from different sources and combine, enrich and analyse these data, and thus share the compiled profiles with an undetermined number of third parties. The purpose of this processing is purely commercial. The infringement that is made with this is entirely disproportionate to that purpose. It also holds that the purpose, of successful advertising, can be achieved by other means that are less detrimental to the data subjects.

4.6.2.4 Conclusion regarding lawfulness

407. From the foregoing, it follows that Oracle and Salesforce do not meet the requirements in order to be able to claim consent as a basis for processing. In addition, the Foundation reiterates that

[273] EDPB Guidelines 05/2020 Consent, p. 22-23.
[274] EDPB Guidelines 05/2020 Consent, p. 23-24.
[275] EDPB Guidelines 05/2020 Consent, p. 24.
[276] HR 9 September 2011, ECLI:NL:HR:2011:BQ8097 (*Santander*), paragraph 3.3.

the duty and burden of proof in order to show that all of the requirements are met rests on Oracle and Salesforce.[277] For this purpose, referring only to compliance documentation on this point is not enough. Now that Oracle and Salesforce are placing the cookies, they will have to demonstrate that consent has actually been obtained from the data subjects whose data they collect and that this consent complies with all applicable requirements.

408. Oracle and Salesforce thus act contrary to the principle of lawfulness of the GDPR (Article 5(1)(a) and(6)), now that they have no adequate basis for processing. Furthermore, they act thus in breach of Article 11.7a Tw. After all, they place cookies on the end-user devices and read information from them, and do not obtain valid consent for this. Acting contrary to the GDPR and Tw (also) qualifies as acting contrary to a legal obligation and therefore delivers an unlawful act towards data subjects.

4.6.3 Processing not transparent

409. Furthermore, Oracle and Salesforce do not provide sufficient information about their processing in order to meet the GDPR requirements. In this way they also act in violation of the GDPR and Tw.

410. Transparency is a fundamental principle for the protection of personal data contained in Article 5(1)(a) GDPR.[278] The requirement of transparency is also the basis of the above-described requirements for informed consent, but has a wider application. It applies to any processing, independently of the basis. The requirement to provide information on the use of cookies also applies in accordance with the GDPR under Article 11.7a(1)(a) Tw.

411. Transparency has long been a core principle of EU law.[279] Transparency should ensure that citizens have confidence in the processes that affect them, helps them to understand those processes and enables them, if necessary, to raise objections. Transparency is also an expression of the principle of fairness in relation to the processing of personal data as contained in Article 8 of the Charter, and is therefore an essential fundamental principle. Transparency as a fundamental aspect of the principles has therefore been added to the provision in Article 5(1)(a) GDPR that data must be processed in a lawful and fair manner.[280]

412. Transparency is intrinsically linked to the fair conduct and accountability of Article 5(2) GDPR. The controller must therefore, inter alia, be able to prove that personal data regarding the data subject are processed in a transparent manner.[281]

413. The requirement of transparency has several aspects, including providing information on the processing of personal data, giving effect to the rights of data subjects and the obligation to

[277] See EDPB Guidelines 05/2020 Consent, par. 36 and 104.
[278] Working Party Article 29, Guidelines on transparency under Regulation (EU) 2016/69, 29 November 2017, as recently amended and adopted on 11 April 2018, WP260rev.01 and as endorsed by the EDPB on 25 May 2018 ('WP260 Transparency'), p.5, par. 2.
[279] Article 1 of the Treaty on European Union ("TEU**")** states that decisions "are taken as openly as possible and as closely as possible to the citizen"; Article 11(2) TEU reads as follows: "The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society"; and Article 15 of the Treaty on the Functioning of the European Union (TFEU) stipulates, inter alia, that EU citizens have a right of access to documents of the institutions, bodies, offices and agencies of the Union, with the aim that these institutions, bodies, offices and agencies of the Union ensure transparency in their work.
[280] In the Data Protection Directive (Directive 95/46/EC), transparency was only mentioned in recital 38, as part of the requirement for processing data in a proper way, but not explicitly in the corresponding Article 6(1)(a).
[281] See also WP260 Transparency, p. 5.

report data leaks. For this case, the first aspect is of particular interest, providing information on the processing of personal data. The obligations in this respect are detailed in, inter alia, Articles 12, 13 and 14 and recital 39 of the GDPR.

414. Recital 39 reads:

> *"Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. […]"*

4.6.3.1 General requirements for transparency

415. Article 12 of the GDPR contains a number of general rules concerning the provision of information to the data subject. The information is required in any case to be in a concise, transparent, intelligible and easily accessible form, using clear and plain language and can be provided electronically. According to recital 58, this applies particularly to situations in which, due to the large number of actors and the technological complexity, it is difficult for a data subject to understand by whom and for what purpose his or her personal data are collected. Online advertisements are cited here as a specific example in such a situation.

416. The controller must take suitable measures to ensure that the data subject receives the information (Article 12 paragraph 1 GDPR)

417. It has already been addressed above (see, inter alia, marginal 380) that when placing cookies on peripherals of Dutch Internet users, Oracle and Salesforce do not ensure that the data subject receives the relevant information. In many cases, the websites through which Oracle and Salesforce place their cookies do not refer to Oracle and Salesforce or their documentation on the processing of personal data. The applicability of the available privacy documentation of Oracle and Salesforce is therefore unclear in itself.

418. In connection with this, it is noted that Oracle mainly provides the information concerning its DMP activities in the Privacy Policy for Oracle Data Cloud[282] and the Privacy Policy for AddThis[283] (see Section 4.3.1.1).

[282] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 21 July 2020 (also **Exhibit 22.a**).
[283] https://www.oracle.com/legal/privacy/addthis-privacy-policy.html, consulted on 23 April 2020.

419. For Salesforce it holds that the privacy documentation on the Dutch-language Salesforce website contains hardly any information about the DMP activities (see Section 4.3.1.2). The English-language version of the website contains the Salesforce Audience Studio Privacy Policy,[284] which provides more information. However, when visiting the Salesforce website, a Dutch Internet user is not redirected to the English-language page of the website. A Dutch Internet user will never see the Audience Studio Privacy Policy, while Salesforce does actually collect data under the scope of its DMP service which are aimed at Dutch Internet users and which are composed in Dutch.

Not concise, transparent and intelligible

420. The information provided by Oracle and Salesforce is not concise, transparent and intelligible. WP29 clarifies in the guidelines relating to transparency that this also entails that controllers must provide the information efficiently and concisely in order to avoid information overload.[285] These requirements are not fulfilled.

421. Processing personal data during the online advertising process is characterised by obscurity and a lack of clarity due to the quantity of parties involved, the purposes for which data are processed, and the unexpected combination of large quantities of personal data from different sources. This obscurity and lack of clarity also characterises the information which is provided under this scope to data subjects. At best, Internet users are first informed by means of a cookie banner on the website that they can subsequently click through via the Partner Cookie Policies to the privacy documentation of Oracle and Salesforce (marginal 381). There is no question of conciseness here, if only due to the fact that this involves multiple layers in which a large quantity of information is given.

422. Both Oracle and Salesforce, for example, indicate that they make use of data partner ShareThis. ShareThis provides some social media share buttons and simultaneously collects personal data that are used for personalised advertising. If a data subject comes onto a website that uses ShareThis buttons, the data subject will need to navigate to that website's privacy policy or cookie policy. In some cases, there is then a hyperlink to the detailed privacy statement of ShareThis.[286] In the privacy statement of ShareThis, under the heading “Data Sharing or Disclosure, Recipients of Your Data”, it is indicated that the customers are, inter alia, Advertisers, Publishers, Data Management Platforms, advertising technology partners and data brokers. ShareThis then mentions that these parties are independent controllers and, as an illustration, refers to the privacy statements of some of its customers:

[284] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 23 April 2020 (also **Exhibit 23.d**).
[285] WP260 Transparency, p. 7 par. 8.
[286] ShareThis, *Privacy,* 28 July 2020, can be consulted via: https://sharethis.com/privacy/.

> Where the GDPR applies to Usage Data and Profile Information and we share this data with our Customers, our Customers are independent controllers in relation to their processing of such data and they process it in accordance with their own privacy policies.
>
> Customers may share the data which they process with other third parties who are not mentioned in this Privacy Notice, in accordance with their own privacy policies. As an example, they may use third party service providers to display advertising or other content on their behalf.
>
> Please review some of our Customer's privacy policies for more information:
>
> LiveRamp: https://liveramp.com/privacy/
> AppNexus: https://www.appnexus.com/platform-privacy-policy
> Eyeota : https://www.eyeota.com/privacy-policy
> Oracle: https://www.oracle.com/legal/privacy/privacy-policy.html
> Lotame: https://www.lotame.com/about-lotame/privacy/
> Nielsen: https://www.nielsen.com/ssa/en/legal/privacy-policy/

423. Oracle is mentioned here, but not Salesforce.[287] The data subject now no longer has a complete picture of the parties who have access to his personal data. If the data subject subsequently wants to know how Oracle processes his personal data, he can click on the link behind Oracle. However, this link leads to the wrong privacy policy, namely the General Privacy Policy of Oracle. The Oracle General Privacy Policy does not contain a description of the processing at issue here. That is described in the Privacy Policy for Oracle Data Cloud. The data subject himself cannot, or can hardly, discover that and therefore never gets the right information about the processing of his personal data by Oracle.

424. It is also striking that ShareThis does not mention Salesforce, while Salesforce indicates that it makes use of ShareThis as a partner. Furthermore, it is striking that ShareThis designates its customers (so also including Oracle) as independent controllers, while Oracle and Salesforce try to take the position that they are merely processor.[288]

425. By this method of informing, data subjects are unable to determine in advance the scope and the consequences of the processing and are surprised later on by the other ways in which their personal data are used. WP29 emphasises that when it concerns complex, technical or unexpected data processing, a separate explanation must also be given in unambiguous wording over what the most important consequences of the processing operation will be. A description must be given of which effect a specific processing operation, which is described in the privacy documentation, will have on a data subject.[289] This should really occur in either the first or the second information layer.

[287] Research by Cookiebot shows that the number of parties with which ShareThis shares data is significantly larger; for this, see Cookiebot, "Ad Tech Surveillance on the Public Sector Web", 2019, can be consulted via: https://www.cookiebot.com/media/1136/cookiebot-report-2019-ad-tech-surveillance-2.pdf.
[288] ShareThis, *Privacy,* 28 July 2020, can be consulted via: https://sharethis.com/privacy/.
[289] WP260 Transparency, p. 8.

426. Another example of this is the process of cookie syncing. Oracle and Salesforce exchange Cookie IDs on a large scale with other parties in the AdTech market, as described in Section3.2.6. By exchanging Cookie IDs, all these AdTech parties can communicate with each other about the data subject, and where necessary exchange even more personal data. Oracle and Salesforce do this on a large scale, as is evident from the research of Dr. Bashir (**Exhibit 16**).

427. Via the 28 websites (of the 100 popular Dutch websites tested) on which Oracle cookies were present, Oracle synchronises cookies with 12 parties. As explained in the facts (marginal 138), it concerns, inter alia, other data brokers and DMPs, including Salesforce, as well as ID5, which is specialised in efficient cookie synchronisation on a large scale. Oracle mentions nothing of the use of this - in the RTB market essential - technique and the parties with whom the personal data, at least Cookie IDs, are shared.

428. Via the 31 websites (of the 100 popular Dutch websites tested) on which Salesforce cookies were present, Salesforce synchronises cookies with 23 parties. As explained in the facts (marginal 140), here too it concerns other data brokers and DMPs, including Oracle and Google. Salesforce also makes no mention whatsoever of the use of this technique and the many parties with whom personal data are exchanged.

429. This has an unforeseeable effect for data subjects, particularly not because it is not made clear just how comprehensive the processing operations, datasets and profiles are, which parties are all involved and how much data is combined together. Instead, the data subject is misled due to the opposite impression being created: examples are given which imply that it involves obvious one-on-one offers that are the clear result of an action carried out by the party which is now making a similar offer. The following is written in the Privacy Policy for Oracle Data Cloud:

> *"iii. So that our Oracle Data Cloud customers are able to personalise their products and services, including site optimisation, email personalisation and optimisation of dynamic marketing and advertisements.*
>
> *Example: If you previously showed an interest in a trip to Hawaii and you subsequently visit the website of a travel agency, then the travel agency can show tailor-made offers for holidays to Hawaii on the homepage."*[290]

430. In no way whatsoever is it clear that this offer is the consequence of the aforementioned processing operations, which contain among other things that data shared from different sources are combined and data are shared with different parties. The most important information, namely that data are collected, combined and enriched from different sources, analysed, and subsequently shared with an unknown number of third parties for advertising purposes, is not provided in a concise, transparent or intelligible manner.

431. Moreover, that this also involves profiling should be explicitly stated, as follows from recital 60 GDPR:

[290] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under '5. Why and how we use your personal information?: A) To enable customers and partners of Oracle Marketing & Data Cloud to market products and services on the basis of your interests, I', consulted on 21 July 2020 (also **Exhibit 22.a**).

[…] "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling." […]

No clear and plain language

432. There is also no question of the use of clear and plain language. Use is made of non-concrete sentence constructions. WP29 finds as follows in respect of the use of language:

> *"Constructions or words such as "can", "could", "certain", "often" and "possible" should also be avoided. When controllers choose to use vague language, then they should be able to show, in accordance with the principle of accountability, why the use of such language cannot be avoided and how the language used does not undermine the fairness of the processing. Paragraphs and sentences should be well constructed, whereby bullets or indents are used to indicate hierarchical relationships.*
>
> *Verbs should be used in the active form and not in the passive form, and superfluous nouns should be avoided. The information which is provided to a data subject should not contain language and terminology that is too legal, technical or specialist. When the information is translated into one or more other languages, the controller is responsible for ensuring that all translations are correct and that the vocabulary and syntax are correct in the other languages, in order that the translated text makes sense and is intelligible. (When the controller addresses data subjects who speak a different language, a translation must be provided in those languages.)"*[291]

433. In the Salesforce Audience Studio Privacy Policy, much use is made in this document of constructions and words which, according to WP29, should be avoided. An example of this is in the following passage (Lawyer's underlining):

> *"The Customer typically uses this data on our Platform to deliver targeted advertising campaigns both on the Customer Site and App as well as off their sites and apps. For example, Customers may use the Platform to help them find interested users and to deliver ads that attempt to bring those users back to the Customer's Site and App. Where our systems can reasonably infer that a particular computer and/or mobile device belong to the same user or household, we may store such information for use on the Platform. The data stored on our Platform may be combined with third-party data (for example, geolocation data provided by a vendor) in order to better target advertisements, to enable Customers to better understand users across multiple computers and devices, and for ad delivery and reporting purposes."*[292]

434. Also in Oracle's Privacy Policy for Oracle Data Cloud[293], use is made of such vague constructions and words and technical and specialist terminology that the data subject can in no way precisely see which of his data are used for which purposes and by which parties.

---

[291] WP260 Transparency, p. 10-11.
[292] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under 'How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform', consulted on 21 July 2020 (also **Exhibit 23.d**).
[293] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 21 July 2020 (also **Exhibit 22.a**).

435. An example of this is in the following passage (Lawyer's underlining):

> *"iii. In order that our Oracle Data Cloud customers can personalise their products and services, including site optimisation, email personalisation and optimisation of dynamic marketing and advertisements.*
>
> *Example: If you previously showed interest in a trip to Hawaii and you subsequently visit the website of a travel agency, the travel agency can show tailor-made offers for holidays to Hawaii on the homepage.*
>
> *iv. For coupling profiles and interest segments so that customers and partners of Oracle Marketing & Data Cloud can couple your interest segments in the different browsers and/or devices which you can use for the purposes described in this section.*
>
> *Example: You are interested in holidays which are offered by a travel agency and you clicked on an online advertisement. You are signed in to multiple devices (your desktop computer, smartphone and tablet) using the same registration. Oracle partners have established that you are probably the same user on these devices. The travel agency can show you holiday offers on these different devices (via an unidentifiable cookie ID)."*[294]

Not easily accessible

436. The requirement that the information should be easily accessible entails that the data subject does not need to go looking for the information themselves. It should be immediately clear to the data subject where and how the information can be found.[295] Furthermore, it is evident from Articles 13 and 14 GDPR that the controller must *provide* the information referred to there. This means that the controller must take active steps to provide the information to the data subject or must actively direct the data subject to the location of the information. It should not be the case that data subjects have to go in search of the relevant information themselves.[296]

437. As already explained above in the context of consent, the information concerning Oracle and Salesforce is not easily accessible.

438. That is because, to start with, Oracle and Salesforce primarily delegate to their customers the obligation to inform Internet users about the processing by Oracle, Salesforce and all other AdTech parties concerned.

439. Salesforce does that as follows:

> ***"Notice to Customer's Users***

[294] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under '5. Why and how we use your personal information?: A) To enable customers and partners of Oracle Marketing & Data Cloud to market products and services on the basis of your interests, I", consulted on 21 July 2020 (also **Exhibit 22.a**).
[295] WP260 Transparency, p. 8 par. 11 and p. 21 par. 33.
[296] WP260 Transparency, p. 21 par. 33.

Customer is required to clearly and conspicuously post notice (e.g., in its privacy policy) to customer's users regarding customer's relationship with Salesforce and other third-party advertising technology companies. Such notice must contain a link to the consumer opt-out mechanism relevant in each jurisdiction, such as the applicable NAI- or DAA-compliant consumer opt-out mechanism."[297]

440. Furthermore, in the best case, data subjects are sent via a cookie banner and the Partner Cookie Policy to the privacy documentation of a large number of third parties involved, including Oracle and/or Salesforce. There they subsequently have to search for the information relevant to them (marginals 381 and further). Insofar as such a structure does actually fulfil the requirement for accessibility, in case of a layered structure it applies that information must be given in the first information layer – in this case, therefore, the cookie banner – concerning the identity of all joint controllers and all purposes for which they process.[298]

441. The cookie banner must also contain information about the enrichment, combination, profiling, sharing and providing of data, since the data subject will not be expecting that without that information and precisely these processing operations (as well as the scale of those) have the greatest effect on the privacy of the data subjects. In addition, the cookie banner must contain information about the rights of the data subjects.[299] This is not how the provision of information is set up in practice. The cookie banner does not contain such information and the data subject is first required to click a few times further before they eventually arrive at such information.

442. A good example of how inaccessible the relevant information is, is the information about sharing data by means of cookie syncing, an essential part of the DMP services of Oracle and Salesforce (for this, see Section 3.2.6):

443. An Internet user who searches for information about the sharing of data by Salesforce will probably find nothing, since the privacy documentation intended for data subjects does not contain this information. Information about this can be found only in the "Audience Studio Notices and License Information" aimed at the customers of Salesforce, and which is only available on the English-language website of Salesforce (**Exhibits 23.e and 23.f**). The Dutch Internet user who searches for information about the processing by Salesforce is, however, not redirected to here (for this, see Section 4.3.1.2).

4.6.3.2 Specific information that must be provided

444. Articles 13 and 14 of the GDPR set out which information must be provided. Article 13 GDPR provides for cases in which the personal data are collected directly from the data subject, Article 14 GDPR for cases in which the data are acquired from another source. That these provisions also apply to the requirement of informed consent of section 11.7a of the

[297] https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/audience-studio-notices-and-license-information.pdf, p. 4, consulted on 24 July 2020.
[298] WP260 Transparency, p. 22 par. 36.
[299] WP260 Transparency, p. 22 par. 36.

Telecommunications Act, is also evident from the aforementioned *Platnet49* ruling of the CJEU:

> *"76 It should be commented in connection with this that Article 10 of guideline 95/46, reference to which is made in Article 5, paragraph 3, of guideline 2002/58 and Article 13 of regulation 2016/679, contains a list of the information which must be provided by the controller to the data subject from whom they acquire the data concerning that data subject themselves"*[300]

445. The first layer of information that is used to inform data subjects should contain, according to the European regulators, the following information:

a. Details of the purpose of the processing;

b. The identity of the controller; and

c. A description of the rights of data subjects.[301]

446. This information must be brought to the attention of the data subject directly on the collection of the data. In addition, on grounds of the principle of fairness, the first layer of information must refer to the processing operations which have the greatest effect on the data subject and which could be unexpected for the data subject. On the basis of that information, the data subject should be able to understand the consequences of the processing.[302]

447. It was already discussed above that the cookie banners on the websites via which Oracle and Salesforce cookies are placed do not contain such information (**Exhibit 28**).

448. Insofar as is relevant here, which information must be provided on grounds of Articles 13 and 14 GDPR is discussed below, as well as to what extent Oracle and Salesforce have included this information in their privacy documentation (**Exhibit 22** and **Exhibit 23**). Mainly Oracle's Privacy Policy for Oracle Data Cloud (**Exhibit 22.a**) and Salesforce's Audience Studio Privacy Policy (**Exhibit 23.d**) were reviewed, since those documents contain the greatest amount of information about the DMP activities. It is emphasised once again that it is not simple for Dutch Internet users to find Salesforce's Audience Studio Privacy Policy (see Section 4.3.1.2). In fact, Salesforce provides *no* information thereby about its DMP processing operations to Dutch Internet users. Therefore, the following applies only insofar as the Salesforce Audience Studio Privacy Policy document shown on the English page must be seen as privacy information within the meaning of Articles 13 and 14. Also for Oracle, it holds that the following applies only insofar as they can demonstrate that the Privacy Policy for Oracle Data Cloud has been effectively (e.g. by means of a link) provided to data subjects.

<u>The identity and the contact details of the controller and, where applicable, of the controller's representative</u>

449. Information concerning the identity of the controller must be provided in such a way that the controller can easily be identified.[303] Oracle and Salesforce are not easily identifiable as such.

[300] CJEU 1 October 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[301] WP260 Transparency, p. 22 par. 36.
[302] WP260 Transparency, p. 22 par. 36.
[303] WP260 Transparency, p. 41

After all, they are never named in the first layer of information. Nor is it made clear that this involves joint responsibility, while that has an extraordinarily significant effect on the far-reaching consequences of the processing.[304]

450. Oracle asserts that it is processor in respect of part of its services (see marginals 272 and 273). However, for which processing operations it designates itself as processor and for which as controller is impossible to decipher from its privacy documentation. Moreover, it has already been shown that Oracle is the controller. Therefore, it should represent itself as such to data subjects.

451. Contrary to its assertions, Oracle designates itself as controller in its privacy documentation. It points to different parties as being controller (see also Section 4.4).[305]. It is not clear thereby who is responsible for which processing operations.

452. Salesforce appears to designate itself wrongly as solely being processor. That only follows from the fact that on the English privacy page (**Exhibit 23.c**), it has included the Audience Studio Privacy Policy (**Exhibit 23.d**) (called Salesforce DMP Privacy Policy) under the heading "Resources in respect of how we protect our customer's data as a processor". This is therefore a page to which the Dutch Internet user will *not* be redirected.

453. Insofar as Salesforce may argue that this also follows from the designation of the controller in its general privacy statement (**Exhibit 23.b**),[306] it applies that what is included there is far too vague to be designated as such for this, see marginals 240 to 243 inclusive). Moreover, since the document then contains a few points of information concerning the DMP service (see Section 4.3.1.2), Salesforce creates the impression that it certainly does designate itself as controller of those processing operations. It is not clarified which Salesforce entity is, in fact, controller thereby.

454. There is no question whatsoever of clear information which makes the controller easily identifiable, not even when the data subject finally reaches the privacy documentation of Salesforce.

<u>The contact details of the data protection officer, where applicable;</u>

455. Salesforce provides no information in its Audience Studio Privacy Policy about a data protection officer, while such an officer is, in view of its activities, obligatory on grounds of Article 37 GDPR. For the rest, according to its general privacy statement, it appears that Salesforce has, in fact, appointed such an officer.[307] It is remarkable that Salesforce does not mention the latter in its Audience Studio Privacy Policy.

<u>The purposes of the processing and the basis of the processing and, if an appeal is made to an interest justified by the basis, the justified interests to which the controller appeals;</u>

456. Oracle only provides very general information about purposes.

---

[304] Cf. WP260, Transparency, p. 22 par. 36.
[305] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "2. Scope" and "3. Who is responsible for the processing of your personal information?", consulted on 22 July 2020 (also **Exhibit 22.a**).
[306] https://www.salesforce.com/nl/company/privacy/full_privacy/, consulted on 22 July 2020 (also **Exhibit 22.a**).
[307] https://www.salesforce.com/nl/company/privacy/full_privacy/, under "13. The "Salesforce Data Protection Officer" is called "Contact us", consulted on 22 July 2020.

457. In Oracle's case, up to 11 June 2020 the purpose of the DMP processing (where relevant) was described in respectively the Dutch and the English versions as follows:

> *"We use your personal data for the following purposes:*
>
> *a) so that customers and partners of Oracle Marketing & Data Cloud can offer you their products and services based on your interests"*[308] **(Exhibit 22.a)**
>
> *"We use personal information for the following commercial purposes:*
>
> *a) to help enable Oracle Marketing & Data Cloud customers and partners to market products and services to you based on your interests"*[309] (**Exhibit 22.d**)

458. Who the "customers and partners" are, which data are used, how data are used and whether the processing is limited to the use of "your interests" is unclear.

459. Oracle changed the English version on 11 June 2020, after receipt of the Foundation's written warning.[310] Specifically, the change concerns a specification of the marketing purpose. But the purpose is still defined very vaguely. Thus, the data processed in this context by Oracle can be used, for example:

> *"to create, communicate, deliver, and exchange offerings that have value for customers, clients, partners and society at large"*
>
> or
>
> *"to encourage safe practices and trends and the provision of factual information, including, by way of example, providing product or automotive recall notices"*[311] **(Exhibit 22.c)**

460. Interestingly, the Dutch version does not (yet) contain this change.[312]

461. In both the English and Dutch versions of the Privacy Policy for Oracle Data Cloud, there then follows a completely different list of purposes which appear to be related to marketing.[313] The privacy documentation does not state which data are used for which purpose.

---

[308] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "5. Why and how we use your personal information?" at "a) To help enable customers and partners of Oracle Marketing & Data Cloud to market products and services to you based on your interests", text up to 11 June 2020. , consulted on 22 July 2020 (also **Exhibit 22.a**).
[309] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "5. For what commercial or business purpose do we use your personal information?", text until 11 June 2020. , consulted on 23 April 2020.
[310] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html , under "5. For what commercial or business purpose do we use your personal information?", consulted on 21 July 2020.
[311] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#scope, under "5. For what commercial or business purpose do we use your personal information?" at "a) To help enable Oracle Marketing & Data Cloud customers and partners to market products and services to you based on your interests", consulted on 23 July 2020.
[312] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 21 July 2020 (also **Exhibit 22.a**).
[313] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "5. For what commercial or business purpose do we use your personal information?" after "More specifically, Oracle can process information about you:"; https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "5. Why and how we use your personal information?" by "a) To help enable customers and partners of Oracle Marketing & Data Cloud to market products and services to you via online and offline marketing activities based on your interests", consulted on 23 July 2017 (also **Exhibit 22.a**)..

462. In its Audience Studio Privacy Policy, Salesforce provides no information whatsoever about purposes, but only gives a few examples of purposes for which it could use its customer data:

> *"The Customer typically uses this data on our Platform to deliver targeted advertising campaigns both on the Customer Site and App as well as off their sites and apps. For example, Customers may use the Platform to help them find interested users and to deliver ads that attempt to bring those users back to the Customer's Site and App. Where our systems can reasonably infer that a particular computer and/or mobile device belong to the same user or household, we may store such information for use on the Platform. The data stored on our Platform may be combined with third-party data (for example, geolocation data provided by a vendor) in order to better target advertisements, to enable Customers to better understand users across multiple computers and devices, and for ad delivery and reporting purposes."*[314]

463. The description of the core of the service therefore remains limited to the comment that customers *mostly* use the service for personalised advertising. This purpose is too general in its formulation and leaves room for other purposes, which are not named.

464. Furthermore, Salesforce provides no information whatsoever about profiling, while they are required to do that (recital 60 GDPR).

465. Oracle and Salesforce are also unclear as to the basis.

466. Insofar as Oracle does designate itself as controller, it indicates that consent is the basis and that this is acquired on behalf of Oracle.[315] However, Oracle indicates that the partners, from which it acquires the data, do not always have a relationship with the data subject.[316] Without further explanation, which is lacking, it is incomprehensible how these partners, who have no relationship with the data subjects, acquire consent.

467. Salesforce provides in its Audience Studio Privacy Policy in respect of the DMP processing no information concerning the basis or bases.[317] Nor is any clear information on this point included in its general privacy policy. Insofar as that policy contains information on the basis of displaying personalised advertisements and content, it merely relates to personalised information about Salesforce ("personalised information about us"), not on personalised information about third parties, such as for which the DMP data are used.[318]

---

[314] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under "How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform", consulted on 21 July 2017 (also **Exhibit 22.a**).
[315] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under 6 "What is our legal basis for information concerning you in the EU/EEC?", consulted on 21 July 2020 (also **Exhibit 22.a**).
[316] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under 4 "Which types of personal information do we process and from which sources?", under "Offline information" "as well as third parties who possibly have no relationship with you", last consulted on 22 July 2020 (also **Exhibit 22.a**).
[317] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 21 July 2020 (also **Exhibit 23.d**).
[318] https://www.salesforce.com/nl/company/privacy/full_privacy/, under "5. Purposes for which we process Personal Data and the legal grounds on which we base that", consulted on 21 July 2020.

The actual recipients of the personal data, including (joint) controllers, processors and third parties to whom the data will be provided (Article 4 sub 9 GDPR);

468. Oracle only included one general comment about the potential recipients of personal data:

> *"Customers and partners of Oracle Data Cloud, including offerors of digital marketing, advertising agencies, online publishers, affiliated TV providers, platforms on the demand side, data management platforms on the supply side and social media networks."*[319]

469. This list in fact concerns the whole *AdTech* market and all website owners. The number of potential recipients is therefore practically unlimited. Furthermore, it is also unclear which role these parties play. Maybe Oracle can be designated with several of these parties as joint controllers (see also marginal 284).

470. Salesforce does provide information about the sharing of personal data.[320] However, in that information Salesforce implies that it only processes pseudonymised data and only shares that in exceptional cases with parties. This is diametrically opposed to what its DMP service actually comprises: the collection of as much traceable information as possible in order to make this available for a large number of parties. Salesforce does not name any recipients in its privacy policy. Salesforce names no recipients in its privacy documentation and provides no specific information about the sharing of personal data under the scope of marketing activities.

471. Thereby, the Defendants do not fulfil the requirement to provide information about actual recipients of the data. Moreover, this is especially true since precisely this aspect has a huge impact on the privacy of data subjects.

The retention period;

472. Oracle stores the data acquired online, for example by means of cookies, for 13 months after its acquisition. The "offline data", including name, address, email address, telephone number, demographic data, purchase data, business data and "publicly available information" is stored by oracle for up to 5 years after acquisition. This long period is unjustifiable.

473. Oracle lists a few retention periods in its privacy documentation.[321] However, no retention period is cited for the data acquired through the Publishers.

474. Salesforce only reports that the third-party cookies of Salesforce which it places have a lifespan of six months.[322] Nothing is mentioned about the storage period of data that are obtained by cookies or that are traded via the DMP service.

475. The parties therefore do not fulfil the requirement to provide information about retention periods. Given the overall objective of the DMP services of Oracle and Salesforce, the

[319] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#3, under "8. When and how can we share your personal information?" under "Sharing with third parties", consulted on 22 July 2020 (also **Exhibit 22.a**).
[320] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under 'How we Use and Share Personal Data', consulted on 22 July 2020.
[321] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#3, under "7. How long do we store information about you?", consulted on 22 July 2020 (also **Exhibit 22.a**).
[322] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under "HTTP Cookies", consulted on 22 July 2020 (also **Exhibit 23.d**).

collection, combination and making available of as much information as possible, it is moreover plausible that the created data sets are retained indefinitely, with which Oracle and Salesforce also act contrary to the principle of data minimisation (for this, see Section 0).

The categories of personal data which are processed; and

476. Insofar as Oracle and Salesforce do not collect the data directly from data subjects but via a different source, information must be included about the categories of personal data which are processed. In any case, a part of the processing concerns this, since Oracle and Salesforce do not only acquire data through cookies placed by themselves, but also acquire data from suppliers, among others, and, by means of cookie syncing, can create links with data acquired by other parties (Sections 3.2.4 to 3.2.6 inclusive).

477. Oracle lists a large number of categories of personal data, which are so broadly formulated that virtually all data fall under those categories.[323]

478. Salesforce only provides a limited description in its privacy documentation of which data it collects. Attention is given, for example, to IP addresses, device IDs and videos which the data subject has watched.[324]

479. However, Salesforce barely mentions the core of its services, namely collecting data about Internet use, tracking data subjects and acquiring data from data partners. It is impossible on the basis of this privacy documentation for the data subject to estimate which data concerning the data subject Salesforce actually processes.

480. Furthermore, Salesforce does not describe in clear language that it creates new personal data from these data, such as profiles and interest segments.

The source of the personal data

481. Since Oracle and Salesforce also do not collect personal data from data subjects directly but via a different source, information must also be included about the source of the data.

482. The information that Oracle provides about this in its privacy documentation, in view of its working methods, cannot be complete. Oracle has placed a link in its privacy documentation to a list of around 75 data partners.[325] The parties listed in the document are supposed to be the only data suppliers in the EU/EEC.[326] In a press release, however, Oracle indicates, inter alia, that it works with 1500 data partners. (**Exhibit 15**). Research has shown, furthermore, that Oracle couples its cookies to the cookies of other parties, even when these are placed with Dutch users (**Exhibit 16**) (as indicated above, this is called "cookie syncing"). Personal data are exchanged using this link, at least the Cookie ID. Furthermore, it is also possible to exchange more data (see also Section 3.2.6). However, the many parties with which Oracle

[323] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#3, part 4, consulted on 22 July 2020 (also **Exhibit 22.a**).
[324] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, under 'Statistical Identifier', 'Mobile Device Identifiers', 'Viewed Content Data', consulted on 22 July 2020.
[325] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html (also **Exhibit 22.a**); https://www.oracle.com/nl/data-cloud/solutions/data-as-a-service/data-providers.html, consulted on 21 July 2020.
[326] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, consulted on 21 July 2020 (also **Exhibit 22.a**).

couples cookies are not named in the privacy documentation and most are not included in the list of data partners.

483. Salesforce provides no information in its privacy documentation about its data suppliers. As set out above (marginals 379 and further), it is the data subject who is required to follow a circuitous route in order to arrive at the extensive list of data partners. Moreover, there are various lists of data partners on the website, which are partly overlapping and partly different (see marginals 117 and 118).[327]

484. Salesforce also provides no information about the coupling of personal data (including Cookie IDs) to the data from other *AdTech* parties by means of cookie syncing. As is evident from the research, Salesforce also makes use of this function (**Exhibit 16**).

485. It is impossible for the data subject to gain a clear and full picture of the sources from which Oracle and Salesforce acquire personal data.

486. As is evident from the above, Oracle and Salesforce do not provide the information required on grounds of Articles 13 and 14 GDPR.

4.6.3.3 Transparency and joint responsibility

487. Moreover, when a situation involves joint responsibility, the controllers must establish in a transparent manner the responsibilities of each of them in respect of compliance with the obligations under the GDPR (Article 26 paragraph 1 GDPR). That should "mainly" concern the rights of data subjects and the information obligations under Articles 13 and 14. It must be clear which role each of them fulfils and which relationship they have with data subjects. The "essence" of the arrangements between the controllers must be made available to the data subjects (Article 26 paragraph 2 GDPR).

488. Every controller is required to take suitable measures in order to ensure that data subjects are informed in a concise, transparent, intelligible, accessible manner, using clear and plain language (Article 12 paragraph 1 GDPR). Oracle and Salesforce do not fulfil this obligation. As explained above, they do not indicate that the situation involves joint responsibility (within their group, see marginal 283), who the joint controllers are, let alone providing insight into the division of roles. Neither do they take appropriate measures to ensure that the parties from whom they obtain data provide such information.

489. In its letter, Oracle asserted the position that it only works with four carefully selected suppliers of data and that it checks carefully whether those suppliers fulfil the provisions of the GDPR. As already stated above, one of these suppliers in ShareThis (see marginal 113.b and 422 and further). As research shows, ShareThis is a party that collects data in an opaque manner on a large scale.[328] It is therefore impossible to adequately inform about all parties with whom the data is shared via ShareThis, let alone that it is possible to specify how the (joint) responsibility is organised.

[327] https://konsole.zendesk.com/hc/en-us/sections/206625468-Salesforce-DMP-Ecosystem-Partners, consulted on 29 April 2020, and https://www.salesforce.com/products/commerce-cloud/partner-marketplace/, consulted on 29 April 2020.
[328] Ad Tech Surveillance on the Public Sector Web, Report by Cookiebot, recommended by EDRi, March 2019, can be consulted on https://www.cookiebot.com/en/cookiebot-report/.

4.6.3.4 Changes to privacy policies

490. It follows from Article 12 GDPR that the transparency requirements of the GDPR apply during the whole life cycle of the processing. Data subjects must therefore be informed of changes to the information of Articles 13 and 14 GDPR. According to WP29, this means that data subjects must also be informed about changes to the privacy statements.

491. Changes which are "substantial or essential" must be actively communicated to the data subject, namely "communicated in such a manner that most recipients actually take note of those".[329] A change to the purpose of the processing must in any case be designated as substantial and essential according to WP29. Notification of that must take place via a suitable medium, such as email, a paper letter or a pop-up on a webpage.[330]

492. Oracle most recently changed its (English) Oracle Data Cloud Privacy Policy on 11 June 2020, after receipt of the written warning from the Foundation (see marginal 459). Up till then, the purpose was described as "to help enable Oracle Marketing & Data Cloud customers and partners to market products and services to you via online and offline marketing activities based on your interests".[331] In the amended privacy documentation, a number of specifications have been added, such as "to create, communicate, deliver, and exchange offerings that have value for customers, clients, partners and society at large" and "to encourage safe practices and trends and the provision of factual information, including, by way of example, providing product or automotive recall notices".[332] The Dutch Privacy Policy for Oracle Data Cloud has not been amended since 26 July 2019.

493. The changes implemented by Oracle in its privacy documentation are of a substantial nature and must therefore be communicated via a suitable medium to the data subjects. Nothing points to Oracle having done that. Moreover, the new privacy documentation does not clearly emphasise what changes were made. Here too, Oracle violates the transparency requirements, as laid down in the Articles 12, 13 and 14 of the GDPR.

4.6.3.5 Conclusion in respect of transparency

494. In view of the above, Oracle and Salesforce do not fulfil the transparency requirements of the GDPR. Thereby they contravene Article 5 paragraph 1 sub a, 12, 13 and 14 GDPR. This contravention also entails a contravention of section 11.7a of the Telecommunications Act, since Oracle and Salesforce are required on grounds of that section to provide information in accordance with the GDPR about the cookies which they place. Acting contrary to the GDPR and Tw (also) qualifies as acting contrary to a legal obligation and therefore delivers an unlawful act in respect of data subjects.

[329] WP260 Transparency, p. 19
[330] Ibid.
[331] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "5. For what commercial or business purpose do we use your personal information?", text up till 11 June 2020, consulted on 23 April 2020.
[332] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, under "5. For what commercial or business purpose do we use your personal information?", text from 11 June 2020, consulted on 10 July 2020.

4.6.4 Processing contrary to data minimisation

495. From the factual framework, it follows that the actions of Oracle and Salesforce are focused on big data (see Section 3.2). They place cookies, thereby collecting data on virtually every Dutch Internet user, evaluate and enrich the data, create and share profiles and link the data sets with other sets of data through cookies syncing. Everything is aimed at collecting as much information as possible about as many Internet users as possible to use as a basis to show targeted advertisements.

496. This practice is diametrically opposed to the principle of data minimisation and is therefore in conflict with the GDPR, as will be explained in the following.

497. The principle of data minimisation, also referred to as minimum data processing, is included in Article 5 paragraph 1 sub c GDPR:

> *"Personal data must be:*
>
> *c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");"*

498. The principle of data minimisation entails:

a. an obligation to minimum data processing; and

b. an obligation to apply data protection by design and by default.

499. The principle of data minimisation is derived from the requirement of proportionality, which is directly related to the assessment to be carried out in the context of Article 8 of the ECHR as to whether the breach of the fundamental right protected by that provision is necessary in a democratic society.[333]

500. That risks exist, particularly in the area of profiling, of a violation of the data minimisation principle, is emphasised by WP29:

> *"The opportunities offered to the business community by profiling, cheaper storage costs and the possibility of processing large quantities of data, can encourage organisations to collect more personal data than they actually need, in case that might be useful in the future. Controllers must ensure that they fulfil the principle of data minimisation, as well as the requirements of purpose limitation and storage limitation.*
>
> *Controllers must be able to explain and justify clearly why they need to collect and store personal data, or consider using combined, anonymised or (when this offers adequate protection) pseudonymised data for profiling."*[334]

[333] Conclusion AG, Registry of the Supreme Court 23 June 2017, ECLI:NL:PHR:2017:553 (*Family Doctor Association/Association of Health Care Providers for Care Communication*).
[334] WP251 Profiling, p. 13

4.6.4.1 Minimal data processing

501. The principle of data minimisation is addressed in a number of recitals of the GDPR, such as recital 39:

> *"The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This is mainly to ensure that the storage period of the personal data is kept to a strict minimum. Personal data may only be processed if the purpose of the processing cannot reasonably be achieved in another manner. In order to ensure that personal data are kept no longer than necessary, time limits should be established by the controller for erasure or for a periodic review. (...)"*

502. The principle of data minimisation therefore contains a proportionality test. If the processing is not proportional and/or the same purpose can reasonably be achieved in another manner, then the requirement of minimisation has not been fulfilled. That even if a legitimate basis exists, which in this case is not so, the processing must still be necessary for the intended purpose is also shown by a ruling from the Supreme Court in relation to section 8 of the Personal Data Protection Act, which applied at the time, the equivalent of Article 6 GDPR:

> *"3.3. (c) Even when the data processing is in principle permitted on grounds of the limited list given in section 8 of the Personal Data Protection Act, the requirement still applies that the processing must be necessary in view of the described purpose of the processing in the concrete case in question. The existence of a legal defence of justification therefore does not mean that the balancing of interests according to the principles cited above under (a) is superfluous. The circumstances of the case in question must be taken into consideration in this balancing of interests."*[335]

503. As explained above in great detail, the processing carried out by Oracle and Salesforce involves the following:

a. Processing of large amounts of personal data per person (Oracle speaks of 30,000 data points, see marginal 121);

b. A huge group of contributors and/or sources of personal data, comprising the Publishers and suppliers of data;

c. Continuous processing whereby it is unclear to what extent the storage is limited by all of the parties and it is highly likely that the data will not actively be erased by some parties;

d. A huge group of data subjects, namely: everyone who uses the Internet;

e. A large and unlimited group of users of the data, comprising the Publishers who use the data in order to be able to market their advertising space better, advertisers which use the data in order to determine their offers, and intermediaries such as ad exchanges, SSPs and DSPs (see marginal 123);

[335] Supreme Court 9 September 2011, ECLI:NL:HR:2011:BQ8097 (*Santander*).

f. The processing of personal data which according to their nature are sensitive, since they provide an extremely detailed picture of (the behaviour of) the data subjects.

504. Therefore, this involves *data maximisation* instead of *data minimisation*. The Defendants collect and combine as much data as possible, from as many sources as possible concerning as many data subjects as possible and, under the scope of profit maximisation, by as many different parties as possible.

505. Because of that, the processing inherently involves a contravention of the principle of data minimisation. That contravention is not in proportion to the – purely commercial – purpose of Oracle and Salesforce and the other parties involved. Contrary to some other big data applications (for example, in the scientific world), this does not serve any public interest. Even the data subjects themselves gain no advantage from the processing operations. The interests of data subjects in the protection of their fundamental rights and freedoms weigh more heavily than the interests of Oracle and Salesforce.

506. It is generally argued that big data applications cannot easily be reconciled with the principle of data minimisation.[336] After all, big data requires data maximisation. Generally speaking, as much data as possible is collected and is automatically combined and analysed using new technology in order to be able to attach certain conclusions to that or to arrive at certain insights. As the European regulators recognise, the principles for the protection of personal data, such as data minimisation, also apply in full to big data.[337]

507. Moreover, the purpose of effective advertising can also be achieved easily in another manner, with less negative consequences for the rights and freedoms of data subjects. After all, the effectiveness of advertisements and other utterances tuned to behaviour has been the subject of discussion for some time now. Increasing numbers of parties are changing over to advertisements on the basis of the context, for example, of news items whereby the advertisement is placed (see Section 186 and further).[338] Contrary to the forms of advertisements on which the DMP service is set up, virtually no personal data is needed for these forms. The only difference is that the economic interests of Oracle and Salesforce do not benefit from this, since this would make their DMP services unnecessary.

4.6.4.2 Data protection by design and by default

508. The principle of data minimisation is explained in further detail including in Article 25 GDPR:

> *"Data protection by design and by default*
>
> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means*

[336] N. Wolters Ruckert & L. van Sloten, 'Big Data: Big Privacy Challenges', *Computerrecht* 2016/82 and L. Viergever & J. Koëter, 'Is our privacy regulation 'Big data proof'?', *Tijdschrift voor Internetrecht*, 6 December 2012, p. 171.
[337] Article 29 working party, Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 14 September 2014, WP221. ('WP221 Big Data')
[338] For example, the STER already started in 2018 with so-called "No Consent Advertising", see Screenforce, *STER starts no consent advertising on online channels of NPO'*, 18 December 2018, can be consulted via: https://screenforce.nl/ster-start-no-consent-advertising-op-online-kanalen-van-npo/.

for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as minimum data processing, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

[…]"

509. On grounds of Article 25 GDPR the controllers must apply the so-called "data protection by design and by default".

a. Data protection by design means that the controller, when determining the means for processing and during the processing itself, must implement appropriate measures and safeguards into the design of the processing in order to meet the requirements of the regulation. Those measures and safeguards should be aimed at fulfilment of the principles of data protection. The term "data minimisation" is explicitly cited in the text of Article 25. The safeguards and measures that must be included in the design of the processing must, therefore, be aimed at ensuring data minimisation.[339]

b. Data protection by default means that the controller must take measures in order to ensure that the default settings mean that only the necessary data are processed. The measures should wherever possible limit the quantity of data collected, the scale of the processing of that data, the duration of the storage and the accessibility to the data. Therefore, standardly as little data as possible are processed, as briefly as possible, etc., while the data subject may actively choose to allow a more extensive processing.[340]

510. Recital 78 states (Lawyer's underlining):

"The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this regulation are met. In order to be able to demonstrate compliance with this regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection <u>by design</u> and data protection <u>by default</u>.

Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard

EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, ('EDPB 4/2019 DPbDD'), p. 6 par. 7-8.

[340] Cf. Data Protection Authority, Microsoft Windows 10 – The processing of personal data via telemetry, 29 August 2017.

to the functions and the processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard for the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. […]"

511. According to the European regulators, under this scope controllers must first assess whether it is necessary at all to process personal data. They are obliged to find out whether technology, processes or methods exist that would make the processing of personal data superfluous.[341]

512. Important elements to be implemented in the design and default settings according to the European regulators include:

a. Data avoidance: actively avoiding the processing of personal data whenever possible for the purpose of the processing.

b. Relevance: limiting the processing to the data which are relevant for the processing. The controller must be able to demonstrate this.

c. Necessity: each part of the dataset must be necessary for the specified purposes of the processing and data may not be processed if the purpose can be achieved in another manner.

d. Limitation: limiting the quantity of the data collected to what is necessary.

e. Data flow: the data flows must be efficient so that no unnecessary copies of the data are made and no points of data collection are used more than is necessary.[342]

513. By acting in the aforementioned way, Oracle and Salesforce are contravening the obligations of Article 25 GDPR. They should have taken into account, even at the time of setting up the DMP and collecting the data, whether, and if so which, personal data are necessary, and to have limited the collection to that. They do not do that, as is also evident from the facts. They have set up their DMP in such a way that a maximum quantity of data is collected. When placing and reading cookies, cookie syncing and the collection from other sources, at no time is the question asked whether that is necessary. This is also the case with regard to the processing operations which follow. No review is made of the relevance or necessity, let alone whether the processing can be avoided. The data are stored in different places and shared with multiple parties. This also means that the number of persons with access to the data is unlimited.

514. Insofar as Oracle and Salesforce invoke pseudonymisation in this context, the following applies. There is pseudonymisation when data are linked to a pseudonym, such as a number,

[341] EDPB 4/2019 DPbDD, p. 19 par. 69.
[342] EDPB 4/2019 DPbDD, p. 19 par. 71.

rather than for example the name of the data subject. However, in pseudonymisation, that pseudonym is still traceable to an identified or identifiable person. For that reason, it holds that with the use of pseudonymisation, there are still personal data.[343] However, pseudonymisation can generally be regarded as a wise security measure, because pseudonymised data can be less easily abused by third parties.

515. In the case of Oracle and Salesforce, and other parties in the RTB market, it holds that they generally invoke pseudonymisation and similar techniques such as hashing, e.g. transforming an IP or email address into a series of numbers, letters and/or other characters. In this way, they try to give the impression that there is no question of personal data or that the privacy is thus protected. This is however not at all the case. Even when using such techniques, the goal is to link as much data as possible to unique Internet users. In hashing, for example, various AdTech parties use the same hashing technique, so that the data of an Internet user that they have collected can be interlinked. In this way, huge amounts of data are collected about Internet users. Using a pseudonym here is therefore not so much a security measure, but rather the identifier under which all data can be linked together. Presenting this as a security measure, or even as "anonymous data", is incorrect and misleading.

516. To illustrate the above, a publication by Dr. Wolfie Christl is introduced into the proceedings as **Exhibit 29**.[344] In this publication, he discusses how pseudonymisation is used, inter alia, in the online advertising market and how Oracle makes use of this in the context of its DMP.

517. No evidence can be found that the default settings applied by Oracle and Salesforce are at any time aimed at limiting the processing or a privacy-friendly approach. Oracle and Salesforce collect as much data as possible by default, and use that data for compiling detailed profiles as standard. Oracle and Salesforce standardly share the data with a large group of users. Therefore, there is no question of data protection by design or by default.

4.6.4.3 Conclusion in respect of data minimisation

518. In view of the above, Oracle and Salesforce do not fulfil the principle of data minimisation and the obligations of minimum data processing and data protection by design and by default. Thereby they contravene Articles 5 paragraph 1 sub c and 25 GDPR.

4.6.5 Forbidden transfer to the United States

519. Oracle and Salesforce provide their DMP service primarily from their head office in the United States, Oracle Corporation and Salesforce.com, Inc. These entities are also the owner of the domains which place BKU and _KUID_ cookies (marginals 296 and 301). They offer their DMPs worldwide. The Dutch entities are also involved in that (marginals 300 and 303). Various different entities in the US are designated as controller in their privacy documentation (marginals 297 and 302). This means that the DMP data are processed in part by Oracle and Salesforce in the US.

[343] See also Working Party Article 29, Opinion 5/2014 on Anonymisation Techniques, 10 April 2014, WP216 ("WP216 "Anonymisation Techniques").
[344] Dr. Wolfie Christl is a respected technology expert, researcher and digital rights activist, see https://wolfie.crackedlabs.org/en.

520. The transfer of personal data from the Netherlands and other parts of the EU to the US by Oracle and Salesforce, as it takes place since 25 May 2018, is unlawful.

521. In its privacy policy Oracle indicates that, insofar as it designates itself as controller, the data are transferred to the US on the basis of the Privacy Shield Decision. However, this decision was recently declared invalid by the CJEU in the *Schrems II* case.[345]

522. Model contracts and binding business conditions of Oracle and Salesforce cannot offer them solace either. After all, these are merely suitable insofar as they would have been processors, while for the DMP activities, they should be considered (joint) controller. Salesforce indicates on its website that, as a result of the *Schrems II* ruling, it makes transfers on the basis of model contracts and binding business conditions, but that does not make the transfer lawful.[346]

523. Even if Oracle and Salesforce perform certain actions as processor, the transfer remains unlawful. After all, from the *Schrems II* case, it is evident that the level of protection in the US is inadequate. Therefore, the model contracts and binding business conditions provide no safeguard for the transfer of data.

524. The following will clarify why Oracle and Salesforce are acting in violation of the GDPR with this transfer. First, the general prohibition on transfer will be discussed. Subsequently, the recent *Schrems II* case will be discussed.

4.6.5.1 Transfer forbidden in principle

525. On grounds of the GDPR, special rules apply to the processing of personal data outside the European Economic Area ("**EEA**") (Article 44 and further GDPR), also referred to as "transfer". "Transfer" is involved when personal data are made known to persons outside the EEA, which is not limited only to storage. Transfer is forbidden unless an exception applies (Article 44 GDPR). The background of this is that many countries offer no suitable protection level for personal data and that the Union Legislator wanted to oblige parties who process data to take account of that.

526. The GDPR offers various mechanisms on the basis of which data may be transferred. The European Commission can, for example, decide that a third country, an area or a sector in a third country safeguards a "suitable protection level" (Article 45 GDPR (a so-called "adequacy decision"). The European Commission determined in 2016 that the U.S. safeguards a suitable protection level for personal data which are transferred from the EU to organisations established in the U.S. when that organisation fulfils the requirements of the EU-US Privacy Shield ("**Privacy Shield Decree**"). [347]

527. When an adequacy decision is lacking, transfer can take place on grounds of suitable safeguards (Article 46 GDPR). One of the "suitable safeguards" concerns the model contracts approved by the European Commission. In 2010 the European Commission approved certain

[345] CJEU 16 July 2020, C-311/18 (*Schrems II*).
[346] https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/EU-Data-Transfer-Mechanisms-FAQ.pdf, consulted on 18 July 2020.
[347] Implementation decree (EU) 2016/1250 of the Commission of 12 July 2016 in accordance with guideline 95/46 on the suitability of the protection offered by the EU-US privacy shield (OJ 2016, L series 207, p. 1, with rectification in OJ 2018, L series 262, p. 90.

model contract provisions ("**Model contract decision**").[348] Another possibility is that the organisation which is at the receiving end of the transfer has so-called "binding business conditions" which are approved by the competent European privacy authority (Article 47 GDPR). The CJEU has confirmed that Articles 44 to 47 of the GDPR implement the express requirement of Article 8(1) of the Charter and are aimed at the high level of protection that the GDPR provides to continue to transfer personal data to a third country.[349]

4.6.5.2 Judgment of the CJEU in *Schrems II*

528. On 16 July 2020, the CJEU gave judgment in the *Schrems II* case about the transfer of personal data from the EU to the US.[350] In that, the CJEU declared the Privacy Shield Decision to be invalid.

529. On grounds of Article 45 paragraph 2 sub a GDPR, the European Commission is required to take into account the following under the scope of taking so-called "adequacy decision" such as the Privacy Shield Decision:

> *"the rule of law, […] concerning among other things national security (…) and the access of government authorities to personal data, […] as well as the existence of effective and enforceable rights of data subjects and effective possibilities to make an administrative appeal or appeal in law for the data subjects whose personal data are transferred."*

530. The CJEU determined that the American surveillance programs[351] do not fulfil the proportionality principle and are not limited to what is strictly necessary.[352] This means that the requirements of Article 45 paragraph 2 sub a GDPR and Article 52, paragraph 1, second sentence, of the Charter.[353]

531. With regard to the access to the court, the CJEU determined that arrangements on which the American surveillance programs are based do not provide any rights to data subjects, which could be enforced by the district courts against the American government authorities, meaning that there is no question of an effective provision in law.[354] The ombudsman mechanism described in the Privacy Shield Decision provides no legal remedy with adequate safeguards as required on grounds of Article 47 of the Charter.[355]

532. With regard to the Model Contract Decree, the CJEU is of the opinion that this can remain intact. However, the transfer of personal data may only take place if the transferring controller and the importing processor offer suitable safeguards, and data subjects have enforceable rights and effective legal remedies available so that the protection level is broadly in line with

[348] Decree 2010/87/EU of the Commission of 5 February 2010 on model contract provisions for the transfer of personal data to processors established in third countries pursuant to guideline 95/46 (OJ 2010, L series 39, p. 5), as amended in the implementation decree (EU) 2016/2297 of the Commission of 16 December 2016 (OJ 2016, L series 644, p. 100).
[349] See CJEU 06 October 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*), paragraph 72
[350] CJEU 16 July 2020, C-311/18 (*Schrems II*).
[351] Based on section 702 of the Foreign Intelligence Surveillance Act, Executive Order 12333 and Presidential Policy Directive 28.
[352] CJEU 16 July 2020, C-311/18 (*Schrems II*), par. 184.
[353] CJEU 16 July 2020, C-311/18 (*Schrems II*), par. 185.
[354] CJEU 16 July 2020, C-311/18 (*Schrems II*), par. 192.
[355] CJEU 16 July 2020, C-311/18 (*Schrems II*), par. 197.

that in the EU.[356] This contains the obligation to take supplementary measures to remedy an inadequate level of protection in a third country.[357]

533. Since the CJEU has determined under the scope of the assessment of the Privacy Shield Decision that the protection level in the U.S. is not adequate, it is hard to see how a transfer to the U.S. on the basis of suitable safeguards, such as model contracts on grounds of Article 46 paragraph 2 sub c GDPR or binding business conditions on grounds of Article 46 paragraph 2 sub b GDPR, is possible. After all, the CJEU determined that, under the scope of the arrangements on which surveillance practices are based, among other things, the protection level in the US does not match that of the EU.

4.6.5.3 Transfer by Oracle and Salesforce unlawful

534. In view of the foregoing, the transfer of personal data by Oracle and Salesforce to the US is in violation of the GDPR, in particular, they thus violate Article 44 and further of the GDPR. Regardless of the role of Oracle, it is moreover clear from the ruling of the CJEU that the level of protection in the US is inadequate. That means that model contracts and binding business conditions cannot provide a safeguard for the transfer of data.

4.6.6 Other violations

535. Besides the principles of lawfulness, transparency and data minimisation discussed above, the GDPR also contains other principles, together with rules based on those. In view of the foregoing, Oracle and Salesforce also act contrary to the principles and rules discussed below.

4.6.6.1 The principle of fairness

536. Article 5(1)(a) GDPR stipulates that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. In the foregoing, it has already been shown that the processing operations performed by Oracle and Salesforce do not comply with the principles of lawfulness and transparency. From the treatment of the principle of transparency, it already followed that the principle of fairness is not satisfied either (Section 0). After all, the principles of fairness and transparency are closely linked.

537. Moreover, it is also evidenced that there is no question of fair data processing, now that Oracle and Salesforce do not conform to the social care requirements (see also Section 5.7.3). The fact that in the context of an unlawful act, a connection must be made with social care in the assessment of the fairness of a processing operation, also follows from the explanatory memorandum to Article 6 of the Data Protection Act, in which the requirement was laid down, that personal data should be processed in a fair and careful manner.

> *"It is more important, in this connection, to look at existing Dutch legislation. The requirement that data should be processed in a fair and careful manner, is more in line with the required social care that one has to observe in order to prevent an unlawful act."*[358]

[356] CJEU 16 July 2020, C-311/18 (*Schrems II*), par. 197.
[357] CJEU 16 July 2020, C-311/18 (*Schrems II*), par. 131.
[358] *Parliamentary Papers II,* 1997-98, 25 892, no. 3, p. 78 (explanatory memorandum).

4.6.6.2 The principle of purpose limitation

538. Article 5(1)(b) GDPR stipulates that personal data that must be collected for specified, explicit and legitimate purposes may not be further processed in a manner that is incompatible with those purposes. This is the principle of purpose limitation. Oracle and Salesforce do not satisfy this principle.

539. The principle of purpose limitation contains two elements. Firstly, data may only be *collected* for specified, explicit and legitimate purposes. It has already been stated that the purposes have not been defined explicitly (marginals 456 and further). Also, it has already been discussed in the foregoing that there is no legitimate basis for the processing by Oracle and Salesforce (Section 0). For this reason alone there can therefore be no question of a legitimate purpose.[359] It is also important here that the purpose that Oracle and Salesforce pursue with the processing is purely commercial and there is no question of any general interest (marginal 180).

540. Secondly, personal data may not be further processed in a way that is incompatible with those purposes. If personal data are further processed for other purposes, then in turn, those new purposes will first of all have to be sufficiently specific and meet the other requirements discussed above. In this case, the data collected are further processed by various other parties, and it is completely unclear to Internet users for what purposes their personal data are being further processed, or even by which parties this is being done.

541. In addition, further processing can only be lawful if it meets, inter alia, the reasonable expectations that the data subject had at the time that his data were collected, and the context in which this happened.[360] The individuals concerned are not at all aware in this case of the scale, the number of players involved in the background and the extent of further processing. This does not, therefore, fall within their reasonable expectations.

542. Various other aspects must also be involved in the assessment as to whether there is a question of compatibility (Article 6(4) GDPR). Among other things, account must be taken of the nature of the personal data and the consequences of further processing for the data subject. In this case, it concerns sensitive personal data that are used to build extremely extensive profiles whose effects on Internet users are unexpected and far-reaching.

543. Also relevant is the relationship between the data subject and the controller. There is no question of a direct relationship between Oracle and/or Salesforce and the Internet user concerned, such as, for example, in the case in which the data of an Internet user are processed by a party from which he has purchased a service or product, for example, a web shop. Indeed, Internet users have no idea whatsoever of the existence of Oracle and Salesforce. Nor is there an equivalent relationship. The Internet user is defenceless against these major players in an international market with a turnover of hundreds of billions.

[359] Working Party Article 29, Opinion 03/2013 on purpose limitation, 02 April 2013, WP203, p. 19 (WP203 Purpose limitation).
[360] WP203 Purpose limitation, p. 12.

544. In view of the foregoing, the processing of personal data by Oracle and Salesforce does not meet the requirement of purpose limitation, neither with regard to the collection, nor with regard to the further processing thereof.

4.6.6.3 The principle of accuracy

545. Article 5(1)(d) GDPR stipulates that personal data must be accurate and must be updated as necessary. Especially when profiling is involved, it is of great importance that the principle of accuracy is satisfied. In this context, the WG29 indicates:

> *"If the data used in an automated decision-making or profiling process is inaccurate, any resultant decision or profile will be flawed. Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Inaccuracies may lead to inappropriate predictions or statements about, for example, someone's health, credit or insurance risk. Even if raw data is recorded accurately, the dataset may not be fully representative or the analytics may contain hidden bias."*[361]

546. In the profiling process, the principle of accuracy should be kept under review at every step, particularly in the case with the following steps, as the WG29 also emphasises:

- collecting data;
- analysing data;
- building a profile for an individual;
- applying a profile to make a decision affecting the individual.

547. According to the WP29, controllers need to introduce robust measures to verify and ensure that data re-used or obtained indirectly is accurate and up to date. This makes it the more important that clear information is provided about the personal data that are processed, so that the data subject can correct errors and improve the quality of the data. In the foregoing, it has already been indicated that no clear information is provided. The process - described in the factual framework - for the collecting and (further) processing of personal data by Oracle and Salesforce, and third parties who have access to the data, makes it impossible to keep the data accurate and up to date. Inherent in the process of data maximisation, profiling and the large-scale sharing of this data, is after all precisely that no more influence can be exerted on the accuracy.

548. Oracle and Salesforce do not therefore satisfy the principle of accuracy.

4.6.6.4 Accountability

549. Article 5(2) GDPR stipulates that the controller is responsible for compliance with the principles regarding the processing of personal data as defined in Article 5(1), namely, the principles of:

[361] WP251 Profiling, p. 13-14.

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Minimum data processing;
- Accuracy;
- Storage limitation; and
- Integrity and confidentiality.

550. Since in view of the foregoing, Oracle and Salesforce act contrary to all these principles, they cannot satisfy their accountability.

551. Article 24 of the GDPR stipulates:

> *"1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*
>
> *2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller."*

552. Recital 75 of the GDPR clarifies that in terms of risks of varying likelihood and severity, various risks for the rights and freedoms of natural persons can result from data processing, which can result in serious physical, material or non-material damage. Subsequently, a number of examples are given of situations in which data processing may result in such damage. This is, inter alia, the case when data subjects are unable to exercise their rights and freedoms, or are prevented from exerting control over their personal data, when special categories of personal data are processed, when there is profiling, when data of vulnerable persons is processed and when there is processing of large amounts of data. All these situations occur in the present case. That means there is a greater duty on Oracle and Salesforce to take appropriate technical and organisational measures to ensure processing in accordance with the GDPR. In view of their practices, this is impossible, and neither is it evident in any way whatsoever that these have been taken.

553. Nor do they meet the specific rules arising from this principle, at least they will have to demonstrate that they satisfy them, such as, insofar as they have not already been discussed in this writ:

- the establishment and implementation of an appropriate data protection policy (Article 24(2) GDPR);
- data protection by design and by default (Article 25 GDPR), it has been shown that such measures have not or have insufficiently been taken;

- the maintenance of a record of processing activities (Article 30 GDPR);
- performing a data protection impact assessment (also called "DPIA") for each processing operation with a high risk for the rights and freedoms of natural persons (Article 35 GDPR) and the prior consultation of the supervisory authority for each DPIA proving that the processing would involve a high risk if the controller does not take measures to reduce the risk (Article 36 GDPR);
- taking additional measures (Article 24(3) GDPR).

4.6.6.5 The conditions for the processing of personal data of children

554. Given the way in which Oracle and Salesforce collect personal data and the volume of the data set, personal data of children are also collected. After all, personal data is processed of practically all Dutch people who read or view information found on the Internet. The GDPR contains additional strict rules for processing the personal data of children.

555. Recital 38 of the GDPR states the following with regard to the processing of the personal data of children:

> *"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child." [Lawyer's underlining]*

556. The GDPR contains several specific rules to ensure this protection.

557. Firstly, Article 12 GDPR stipulates that the information that the data subject should receive should be provided based on the principle of transparency in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *in particular* for any information addressed specifically to a child. Recital 58 clarifies:

> *"Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."*

558. In marginals 432 and further it has been shown that the information supplied by Oracle and Salesforce is not intelligible for adults, let alone children.

559. Secondly, there is a right to be forgotten when personal data are collected in relation to the offer of information society services to a child (Article 17(1)(f) GDPR). Recital 65 of the GDPR illustrates this as follows:

> *"(...) In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the*

processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. (…)"

560. Oracle and Salesforce cannot meet this requirement, as will also be shown below.

561. Thirdly, it is not allowed to take automated decisions as referred to in Article 22 GDPR with regard to children, unless required by necessity (recital 71 GDPR).[362] Such decisions are taken by Oracle and Salesforce, and there is no evidence that children are excluded from this. There is no question of a necessity thereto.

562. In addition, WP29 has indicated that since children constitute a vulnerable group of society, organisations in general should refrain from profiling of children for marketing purposes.[363] Even if, according to your Court, Article 22 GDPR would not apply, it therefore holds that compiling profiles of children by Oracle and Salesforce is not allowed.

563. Fourthly, Article 8 GDPR stipulates that when processing is based on consent, in relation to the offer of information society services directly to a child, this processing is only lawful where the child is at least 16 years old. If the child is under 16, parental consent is required.

564. This means that Salesforce and Oracle require parental consent for children under 16 years of age whose personal data they process, which consent they do not have. After all, personal data are, partly, collected in connection with information society services, i.e. when visiting a website, and in that context the provision of, not legally valid, consent to the processing of personal data. In addition, at least in a (considerable) portion of the websites, there will be a direct offer to a child. This is different only if the provider of information society services makes it clear in this regard to potential users that it only offers its services to persons aged 18 or older, and this is not undermined by other evidence.[364] Of this, at least for some of the websites on which Oracle and Salesforce collect personal data, there is no question.

a. The prohibition on the processing of special categories of personal data and criminal data

565. Article 9 GDPR stipulates that the processing of special categories of personal data is prohibited, unless there is an exception. Special categories of personal data are understood to mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[362] WP251 Profiling, p. 34.
[363] WP251 Profiling, p. 35.
[364] Working Party Article 29, Guidelines for consent under Regulation 2016/679, WP259, p. 29.

566. The prohibition is applicable not only when special categories of personal data are collected directly, but also when profiles are compiled which contain a combination of data from which special categories of personal data can be derived. WP29 describes this as follows:

> *"Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.*
>
> *Correlations may be discovered that indicate something about individuals' health, political convictions, religious beliefs or sexual orientation (...)."*[365]

567. The example has already been cited of the supermarket chain that had discovered that a woman was pregnant before her own father knew it (marginal 55). In this case, there was a question of the processing of special data, namely health information. Also discussed is the research showing that when simple Facebook "likes" were combined with data from other sources, the sexual orientation of male users could be established in 88% of cases, in 95% of cases ethnicity was well estimated, and in 82% of cases the researchers made a correct prediction as to whether the Internet user was Christian or Muslim. All of this also concerns special data, which were derived from a dataset that was far less extensive than the datasets available to Oracle and Salesforce.

568. It must therefore be assumed that Oracle and Salesforce process not only normal personal data, but also special categories of personal data, without an exception to the prohibition being applicable thereto. One of the possible exceptions is explicit consent of the data subject (Article 9(2)(a) GDPR). Explicit consent is a more stringent form of consent, which must meet more requirements than the consent under Article 6 GDPR. There must be an explicit statement by the data subject. Now that the requirements for standard consent under Article 6 GDPR are not met (Section 0), there can also be no question of explicit consent within the meaning of Article 9 GDPR. The other exceptions in Article 9 are not eligible either.

569. Moreover, it holds that under Article 22(4) GDPR, automated decisions referred to in Article 22(1) GDPR may not be based on special categories of personal data, unless an exception applies, which is not the case here.

570. Article 10 GDPR stipulates that personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. This includes both convictions as well as possible legitimate suspicions. Just as with special categories of personal data, the profiles processed by Oracle and Salesforce will include criminal records. Thus, for example by means of cookies, a picture can be obtained of online fraud.

[365] WP251 Profiling, p. 17.

571. The exceptions to the prohibition of the processing of criminal data are contained in Articles 32 and 33 of the Implementation Act of the General Data Protection Regulation ("**UAVG**"). It also holds that one of the exceptions is explicit consent, which exception as discussed above may not be invoked. Nor are any of the other exemptions eligible.

4.6.6.6 Rights of the data subject

572. The GDPR contains a number of additional rights for data subjects, namely:

a. The right to withdraw consent (Article 7(3) GDPR);

b. The right of access (Article 15 GDPR);

c. The right to rectification (Article 16 GDPR);

d. The right to erasure (Article 17 GDPR);

e. The right to restriction of processing (Article 18 GDPR):

f. Notification obligation regarding erasure or restriction of processing by the controller to each recipient of personal data (Article 19 GDPR);

g. The right to data portability (Article 20 GDPR); and

h. The right to object.

573. Data subjects must be actively informed of these rights (Article 12(1) in conjunction with Article 13(2)(b) and (c) and Article 14(2)(c) and (d) of the GDPR). Recital 59 GDPR also emphasises that 'modalities' (arrangements) should be provided for *facilitating* the exercise of the data subject's rights. Regarding the withdrawal of consent, Article 7(3) GDPR stipulates that this should be as simple as giving consent.

574. In Section 0, it has already been indicated that the way in which Oracle and Salesforce provide information does not comply with the requirements of the GDPR. This also applies to how data subjects are informed about their rights. The information discussed below is therefore not communicated correctly to the data subjects.

575. Moreover, it is inherent in the manner in which Oracle and Salesforce process personal data that it is impossible to (fully) comply with (all) rights of data subjects. That is also evident from the privacy documentation of Oracle and Salesforce (**Exhibits 22 and 23**).

576. Neither in the Privacy Policy for Oracle Data Cloud (Chapter 12, "What choices do you have?") nor in the AddThis Privacy Policy (Chapter 7, "What are your privacy rights?") is any information included on the rights listed under a, c and e-h above. Apparently there is no possibility to exercise those rights.

577. However, both chapters make mention of a very complicated way of opting out and objecting to the use of information about a data subject. Three possible opt-out tools are described, one of which relates to an industry solution that does not contain a specific solution for the personal data that is processed by Oracle, and an additional app that has to be downloaded to

a mobile device. In view of the scale on which data are shared, none of these solutions will completely stop the processing. Moreover, the "opt-out tool for Oracle Data Cloud" cannot be used by people in the Netherlands anyway, as will be discussed below. In addition, it was stated that none of the tools work if certain cookies are rejected automatically. In no way are data subjects *facilitated* a way of making an objection. Nor is the information presented clearly and separately from other information, as Article 21(4) GDPR requires.

578. There is also mention of a way to erase data through the opt-out tool for Oracle Data Cloud, one of the tools that is also mentioned among the opt outs. When this is clicked, however, one is redirected through yet another page, to a screen where a plurality of information must be filled in and where, via a drop down menu, the country of the data subject must be selected. It subsequently appears that the tool is only available to people in the United States (**Exhibit 30**). So there is no opt-out or erasure possibility for people in the Netherlands. The screen indicates that no "Offline personal data for interest-based advertising in your region" would be processed, i.e. all countries except the United States. In view of what has been discussed about this above, this is obviously incorrect.

579. That may also be seen from the fact that when using the option to obtain access, results *are* given (**Exhibit 21**). These are not at all complete however, because by no means all information that is to be provided under Article 15 GDPR is included herein.

580. Regarding Salesforce, it holds that in the document "Audience Studio and Data Studio Privacy" (**Exhibit 23.d**) no information whatsoever is included on the rights mentioned under a and e-g above. Apparently there is no possibility to exercise those rights.

581. A notification is made of a browser opt-out, which works by means of a cookie. The result of this is, inter alia, that customers of Salesforce may no longer target Internet users, but this says nothing about the personal data that those customers already have.

582. Regarding the right to access, erasure and rectification, the data subject would have to send an email or a request by mail to an address in the United States. What should be included in the request and how this could lead to granting the request is completely unclear, now that Salesforce claims only to process pseudonymised information and therefore the data subject should not be able to be recognised by means of an email address or name. Probably this is why Salesforce indicates that it may not be able to provide the information. Moreover, it is indicated that the request cannot relate to data stored for customers.

583. In view of the above, Oracle and Salesforce do not fulfil the obligation of giving effect to the rights of data subjects.

4.7 Oracle protects personal data inadequately, according to a data breach in 2020

584. As described above, a data breach occurred at Oracle earlier this year (see **Exhibit 12** and marginal 149.a).[366] A researcher and journalists of technology medium TechCrunch had gained unauthorised access to a server of Oracle, as well as the personal data stored on that. This involved the personal data such as name, address, email address and personal data of a

[366] Techcrunch, *Oracle's Bluekai tracks you across the web. That data spilled online,* 19 June 2020, can be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).

sensitive nature such as concerning participation in online games of chance for e-sports and payment details. This involved data from a huge group of data subjects. Simply due to the size of the accessible database, this data breach was one of the largest data breaches of the year. [367]

585. The researcher and TechCrunch could access the data because the server where the data was stored was not properly secured and, inter alia, no login password was required.

4.7.1 Security obligation

586. On grounds of Article 32 GDPR the controller and processor must take suitable measures in order to protect the personal data which they process.

587. Article 32 GDPR:

> *"Security of processing*
>
> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, […]"*

588. This obligation is a result of the principle of integrity and confidentiality (Article 5 paragraph 1 sub f GDPR) and is addressed in further detail in recital 39. Personal data must be processed in a manner which safeguards a suitable security and confidentiality of those data, partly to prevent unauthorised access to or the unauthorised use of personal data and the devices used for the processing.[368]

589. When third parties are able to gain access to personal data without the authority to process the personal data, as happened here, it is clear that inadequate security measures were taken.[369] That applies all the more since this involved an enormous quantity of data, including data of a sensitive nature such as data concerning the participation in games of chance and payment details. The security level tuned to the risk should therefore have been set relatively high. That such a database is available without login with password is, in connection with this, incomprehensible. That this involved a breach of the security implies, moreover, that the security obligation was violated.

590. That Oracle admitted that, by taking supplementary measures, it was able to prevent the incident from being repeated [370]demonstrates, moreover, that Oracle was able to take measures which could have prevented the incident. Oracle should simply have taken those measures in advance.

---

[367] Techcrunch, *Oracle's Bluekai tracks you across the web. That data spilled online,* 19 June 2020, can be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).
[368] Article 5 paragraph 1 sub f GDPR and recital 39 of the GDPR.
[369] Cf. Data Protection Authority, *Haga Hospital - Decision to impose an administrative fine and an incremental penalty*, 18 June 2020, p. 16, can be consulted via; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf; Data Protection Authority, *UWV – Last onder dwangsom*, 31 July 2018, can be consulted via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/last_onder_dwangsom_uwv_werkgeversportaal.pdf.
[370] Techcrunch, *Oracle's Bluekai tracks you across the web. That data spilled online,* 19 June 2020, can be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).

591. Oracle did not thereby fulfil its obligation to adequately secure the personal data which it processes. This involves a violation of Article 5 paragraph 1 sub f and 32 GDPR.

4.7.2 Data breach is a violation in connection with security

592. Moreover, the incident resulted in a breach in connection with personal data as referred to in Articles 4 paragraph 12 and 33 and 34 GDPR.

593. Article 4 paragraph 12 GDPR:

> *"'personal data breach': a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;"*

594. In the case in hand there was unauthorised access to stored data. That qualifies the incident as being a breach. On grounds of Articles 33 and 34 GDPR, such a breach must be reported:

a. To the supervisory authority unless it is unlikely that the breach will result in risks for data subjects (Article 33 paragraph 1 GDPR); and

b. To the data subjects when the breach is likely to result in a high risk to the rights and freedoms of natural persons (Article 34 paragraph 1 GDPR).

595. Moreover, since it concerns a large quantity of data in the case in hand, including data of a sensitive nature, it seems likely that the breach has resulted in risks for data subjects, and Oracle should have reported the incident to the relevant supervisory authority. For those persons of whom the database contained data of a sensitive nature, it also applies that the breach probably resulted in a high risk. Therefore, these data subjects should also have been informed.[371] It does not appear that Oracle did that.

4.7.3 Conclusion in respect of security

596. It follows from the above that Oracle breached the security obligation of Article 32 GDPR. After all, third parties were able to acquire unauthorised access to the personal data which they processed. This applies even when, as they wrongly assert, they were only processor for a part of the processing. Furthermore, the breach of security should have been reported to the authorities and the data subjects.

597. In view of the above, Oracle does not fulfil the principle of integrity and confidentiality and the obligations in respect of security and data breaches. It contravenes thereby Articles 5 paragraph 1 sub f, 32, 33 and 34 GDPR.

5 LIABILITY AND DAMAGES

5.1 Primary: Liability under the GDPR

598. The Union legislator intends offering citizens by means of the GDPR a high level of protection:

[371] Article 29 working party, Guidelines on Personal data breach notification under Regulation 2016/679, 03 October 2017, last reviewed and approved on 06 February 2018, WP250rev.01, and as endorsed by the EDPB on 25 May 2018; Policy rules 'The duty to report data breaches in the Data Protection Act (WBP)' of 8 December 2015 (*Stcrt*. 2015, no. 46128).

> *"In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States."*[372]

599. The choice for a regulation with direct effect instead of a guideline provides for equal powers in the area of supervision and enforcement and comparable sanctions for breaches of the European privacy legislation in the Member States (Lawyer's underlining).

> *"Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States."*[373]

600. For example, the GDPR obliges all Member States to apply a system which provides for "effective, proportionate and dissuasive" penalties.[374]

601. Violations of the GDPR may be fined, depending on the violation, by amounts up to € 10,000,000 or € 20,000,000, respectively 2% or 4% of the worldwide annual turnover in the previous financial year (Article 83 GDPR). Since the GDPR became applicable, the national privacy supervisory authorities have several times already made use of their capacity to fine within the EU. The French supervisor CNIL imposed a fine of € 50 million on Google LLC, partly due to a lack of transparency and inadequate provision of information.[375] The German supervisor imposed a fine of € 14.5 million on a housing association due to the large-scale storage of personal data of tenants.[376] Halfway through last year the British supervisor, the ICO, announced its intention to impose a fine of € 205 million on the airline company British Airways due to a data breach.[377] In the same week, the ICO announced the intention to fine the Marriott hotel chain more than € 110 million, also due to a data breach.[378] It is expected that several hefty fines will follow in the coming years.

602. The Dutch supervisor, the Data Protection Authority ("**AP**"), has imposed large fines as well. The Haga Hospital was required to pay a fine of € 460,000 because the internal security of the patient files was inadequate. In addition, the Data Protection Authority imposed an order subject to a penalty for non-compliance in order to ensure that the security was brought up to

---

[372] Recital 10 GDPR.
[373] Recital 11 GDPR.
[374] Article 84 GDPR. Cf. also recitals 151 and 152 of the GDPR
[375] Commission nationale de l'informatique et des libertés (CNIL), *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*, to be consulted via: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
[376] EDPB, *Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company*, 5 November 2019, to be consulted via: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en
[377] ICO, *Intention to fine British Airways £183.39m under GDPR for data breach*, 9 July 2019, to be consulted via: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
[378] ICO, *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*, to be consulted via:https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

standard. [379] In March this year the Data Protection Authority imposed a fine on the tennis association KNLTB of € 525,000 for selling personal data.[380] Two months later, an unknown company received a fine of € 725,000 for processing fingerprints of employees.[381]

603. Nevertheless, serious penalties can be counted on the fingers of one hand. That while in 2019, the Data Protection Authority received more than 27,800 complaints of privacy, a substantial increase compared with the previous years.[382] The Data Protection Authority emphasised repeatedly that it has insufficient capacity to ensure the quick handling of all complaints.[383] These capacity problems are also experienced in the rest of Europe. In a recent evaluation report concerning the GDPR, the European Commission expressed its concerns about the adverse effect of this on national enforcement of the rules set out in the GDPR.[384]

604. As a result of the lack of enforcement under public law, in recent years, data brokers such as Oracle and Salesforce have been left undisturbed to further develop products that have been created to exploit as much personal data as possible about as many Internet users as possible. As professor and lawyer Lokke Moerel[385] formulates it aptly:

> *"But the business model of the major technology companies and data brokers has remained largely unchanged. Via cookies, they still collect data to their heart's content, combining them into profiles and selling them to third parties for advertising. The consent that citizens should give for the cookies is a sham, according to Moerel. She speaks of 'widespread non-compliance with the GDPR'."* [386]

605. The national supervisory authorities simply lack the clout to call a halt to this kind of behaviour. A necessary addition to the enforcement under public law is therefore the possibility of tackling privacy breaches based on private enforcement. The GDPR provides plenty of possibilities for this option. Article 80 GDPR gives data subjects the option of having themselves represented by a foundation that exercises certain rights on their behalf and that exercises the right to claim compensation. Article 82 GDPR gives everybody who has suffered damage (incl. harm, losses and injury) as the result of a violation of the GDPR the right to receive compensation from the controller or the processor.

---

[379] Data Protection Authority, *Haga fined for inadequate internal security of patient files,* 16 July 2019, to be consulted via: https://autoriteitpersonal data.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers
[380] Data Protection Authority, *Fine for tennis association for selling personal data*, 03 March 2020, to be consulted via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens
[381] Data Protection Authority, *Fine for company for processing fingerprints of employees*, 30 April 2020, to be consulted via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers
[382] Data Protection Authority, *Large increase in number of privacy complaints in 2019, 14 February 2020*, can be consulted via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019.
[383] See RTLZ, *Privacy authority unable to handle the workload: threat of serious privacy breaches,* 14 February 2020, can be consulted via: https://www.rtlnieuws.nl/tech/artikel/5020511/autoriteit-persoonsgegevens-tekort-drukte-privacyklachten-avg-d66-sp
[384] European Commission, 27 June 2020, 'Staff Working Document: accompanying the Communication - two years of application of the General Data Protection Regulation (COM(2020) 264 final)
[385] Prof. Mr. Lokke Moerel is associated with Tilburg University, see https://www.tilburguniversity.edu/nl/medewerkers/e-m-l-moerel and with international law firm Morrisson Foerster, see https://www.mofo.com/people/lokke-moerel.html.
[386] *Privacy Act still lacks teeth after two years*, Financieel Dagblad 25 May 2020, can be consulted via: https://fd.nl/ondernemen/1345538/privacywet-mist-na-twee-jaar-nog-steeds-tanden.

606. In this way, what is known as 'scattered damage' also qualifies for reimbursement.[387] With this type of damage, the damage per individual case is too small when compared with the costs of legal proceedings.[388]

607. On 1 January 2020 the Settlement of Damages Claims in Collective Proceedings Act came into force. This act makes it possible to commence legal proceedings in a collective claim for damages. This is included in Article 305a Book 3 of the Dutch Civil Code. Further details about this are given in chapter 8.

5.2 Violating the GDPR, accountability and relativity

608. As explained in chapter 4, Oracle and Salesforce act contrary to the fundamental rights of data subjects and they violate the GDPR and Article 11.7a Tw. They do this in particular by:

a. The use of automated decision-making by profiling (Article 22 GDPR);

b. Without a processing basis (in this case: consent), the processing of personal data by, inter alia, placing cookies (Article 6 GDPR and 11.7a TA);

c. Not meeting the requirements for making the processing transparent for data subjects (Article 12 – 14 GDPR and 11.7a TA);

d. The maximisation of data instead of the required data minimisation (Article 5(1)(c) and 25 of the GDPR);

e. The unlawful transfer of personal data to the US (Article 44 and further of the GDPR).

609. Now that Oracle and Salesforce are the controller for this, pursuant to Article 82 GDPR, they are liable for the damage caused by the unlawful processing. Moreover, a relativity requirement is included in the last sentence of Article 82 paragraph 2 GDPR: the GDPR also covers protection against the damage in the manner it has occurred In the following, the foregoing will be explained in more detail.

5.2.1 Basic principle: Oracle and Salesforce are suspected of processing personal data (Article 11.7a(4) Tw)

610. Article 11.7a(4) Tw includes presumptive evidence (Section 4.3.2.2). This presumptive evidence means that if cookies are used to collect, combine or analyse data on the use of various services of the information society, such as websites, so that the Internet user can be treated differently, it is suspected that there is a question of processing personal data.[389]

[387] W.H. van Boom, 'Implementing enforcement in private law', *NJB* 2007/826, issue 16, p. 987; I.N. Tzankova, *Scattered damage*, The Hague: Sdu Publishers 2006, p. 50.
[388] M. Rottenberg & D. Jacobs: 'Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres', in: D. Wright & P. De Hert (ed.), Enforcing Privacy: Regulatory, Legal and Technological Approaches, Springer International Publishing Switzerland 2016, p. 311-312.
[389] *Parliamentary Papers I*, 2011/12, 32549, E; *Parliamentary Papers II* 2013/14, 33902, 3.

611. This presumptive evidence is included because of concerns about the privacy implications of 'third party cookies', as well as about the cookies with which surfing behaviour, interests and other user data are analysed for commercial purposes.[390]

612. In this writ, the Foundation has explained with reasons that the BKU and _KUID_ cookies of Oracle and Salesforce fall perfectly under this presumptive evidence (see Section 4.3.2.2). This means that Oracle and Salesforce are suspected of processing personal data on the basis of the Tw.

613. This presumption means that Oracle and Salesforce should - apart from the rules in Article 11.7a Tw - also comply with the principles of the GDPR.[391]

614. Furthermore, for the BKU and _KUID_ cookies, it holds that research (**Exhibit 16**) shows that Oracle and Salesforce in any case place some of the cookies themselves. Under Article 11.7a TA, there is the obligation to obtain consent and provide information regarding cookies and on the person placing the cookies. Even if under the GDPR, Oracle and Salesforce were only the processor and even if there were no question of processing personal data, then pursuant to Article 11.7a TA, they still bear the burden of proof to demonstrate that informed consent has been obtained and that that consent and information meet the GDPR, because it places the cookies.

5.2.2 Basic principle: Oracle and Salesforce are controllers within the meaning of the GDPR

615. As has already been explained, Oracle and Salesforce process personal data on a large scale for commercial purposes. This means that the personal characteristics and data of everyone who is online are continuously collected and exchanged by and with the aid of, inter alia, Oracle and Salesforce.

616. The basic principle has to be that the person who processes personal data is responsible for the processing, unless he proves that it is not the case.[392] There is a special rule on presumptive evidence that gives rise to a different division of 'the obligation to furnish facts' (*stelplicht*), the burden of proof and/or the evidentiary risk.

617. Now that Oracle and Salesforce process personal data, the basic principle has to be that they are controller. The Foundation does not need to prove this. In Section 4.4, it has sufficiently explained why Oracle and Salesforce are the controller for these processing operations. If Oracle and Salesforce think that they are no controller, they must prove this.

618. The GDPR only defines two roles for parties that process personal data: the controller (Article 4(7) GDPR) and the processor (Article 4(8) GDPR). From the case law of the CJEU, it follows that the concept of "controller" should be interpreted broadly, also taking into account the objective of the GDPR to safeguard a high level of data protection.[393] The EDPS confirms that

[390] *Parliamentary Papers II,* 2011/12, 32549, 39
[391] *Parliamentary Papers II,* 2013/14. 33902, no. 3
[392] Court of 's-Hertogenbosch, 31 January 2013, ECLI:NL:RBOBR:2013:BZ2126; WP29 Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010.
[393] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), paragraph 66; CJEU 10 July 2018, Case C 25/17, (*Jehovan todistajat*), paragraph 66; CJEU 05 June 2018, C 210/16 (*Wirtschaftsakademie Schleswig-Holstein*), paragraph 28; CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain and Google*)

this broad interpretation also serves the objective of avoiding a lack of responsibility and thereby ensuring that data subjects have the guarantee of effective and complete protection.[394] This implies that a party who thinks it is merely processor will have to prove that. This party cannot therefore avoid its accountability with the sole defence that it is not the controller.

5.2.3 Basic principle: the burden of proof of compliance with the principles of the GDPR rests on Oracle and Salesforce

619. Article 5(2) of the GDPR stipulates that the controller is responsible for compliance with the principles of Article 5(1) of the GDPR, including the principles of lawfulness, transparency, minimal data processing, integrity and confidentiality covered extensively in this writ (see Chapter 4). The controller must be able to demonstrate that it satisfies these principles. This is called accountability or the principle of accountability.[395]

620. The principles are also elaborated in the other articles of the GDPR, so that accountability essentially applies to all obligations under the GDPR. Incidentally, this is also confirmed in Article 24 GDPR, from which it follows that the controller must be able to prove that the processing is carried out in accordance with the GDPR. In this context, reference is also made to recitals 74 and 79 of the GDPR, from which it follows that for each processing operation, it should be established who is the controller and that this party must be able to prove that it meets the GDPR.

621. The accountability, or the principle of accountability, of, inter alia, Articles 5(2) and 24 of the GDPR involves a reversal of the burden of proof.[396] This means that it is up to the controllers, in this case Oracle and Salesforce, to demonstrate that they complied with the principles of the GDPR. So the Foundation does not have to prove that Oracle and Salesforce violated the principles of the GDPR. The Foundation, moreover, takes the view that it has already set this forth and demonstrated it sufficiently in Chapter 4 'Privacy Law'. Oracle and Salesforce cannot therefore suffice with a challenge to the allegations and facts of the Foundation. Oracle and Salesforce will have to demonstrate that they complied with the principles of the GDPR, which they will not be able to do successfully, considering the allegations and facts of the Foundation.

622. It further follows from the recitals of the GDPR that in accordance with the principles of proper and transparent processing (Article 5 paragraph 1 (a) of the GDPR) the data subjects must be informed of the fact that processing is taking place and of the purposes of the processing. The controller must provide the data subjects with the more detailed information which is necessary to guarantee to the data subject a proper and transparent processing, with due observance of the specific circumstances and the context in which the personal data are processed. The burden of proof that the controller has complied with the principle of transparency, and so has adequately informed the data subjects, rests with the controller (Article 5 paragraph 2 in conjunction with paragraph 1(a) of the GDPR.[397] In addition, it also holds that the transparency requirement also includes the requirement to be transparent about

[394] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13.
[395] J. Jansen & N.D. Schuitema, 'De AVG en het gebruik van artificial intelligence' (the GDPR and the use of artificial intelligence), *TvCo* 2020/3/4, p. 183.
[396] P.A. Nabben & E.C. Post Uiterweer, 'De AVG: hoe heet wordt de soep gegeten?' (The GDPR: how hot is the soup eaten?), *ArbeidsRecht* 2019/24, p. 24.
[397] See also WP260 Transparency, inter alia par. 2, 13, 21 and 28.

who is the controller and who are otherwise involved (as recipients) in the processing (see Section 0 "4.6.3 Processing not transparent"). It also follows from this that it is Oracle and Salesforce that need to clarify this.

623. Finally, it holds that for the consent required in this context, the GDPR expressly stipulates that the burden of proof rests with the controller to demonstrate that it has obtained consent for the processing (Article 7(1) GDPR).[398]

5.3 Causal link between damage and violation of the GDPR is assumed

624. It follows from Article 82 paragraphs 1 and 2 of the GDPR that the controller is liable in respect of a data subject if an unlawful processing of personal data takes place, irrespective of whether the controller is to be reproached for something. This is why there is said to be a risk liability: the controller is liable in respect of the data subject due to the sole fact that, on the processing of their personal data, the GDPR was infringed, irrespective of whether the controller is in any way culpable with regard to that violation. This interpretation of Article 82 GDPR is widely supported in the literature (see for example Van der Jagt-Vink [399] and Van Schelven[400]). The controller can only be indemnified from liability if he can demonstrate that he is not responsible in any way for the fact causing the damage.[401] As a result of the foregoing, the Foundation does not have to demonstrate causal link. The causal link (CSQN link) has already been assumed by violation of the GDPR by Oracle and Salesforce.

5.4 Involvement alone is enough for joint liability

625. What is new in respect of the Privacy Directive is that the GDPR makes it possible for the data subjects to recover their damage from each of the parties that were involved in the processing in question. After all, it follows from Article 82 paragraph 2 GDPR that *every* controller who is *involved* with the processing is liable for the damage caused by a violation of the GDPR. That the term 'involved' was chosen shows that the threshold for liability is low.

5.5 Right to compensation on the grounds of Article 82 GDPR

5.5.1 Introduction

626. It has been shown in the previous chapters that Oracle and Salesforce breach the GDPR structurally and on a large scale. Oracle and Salesforce collect, enrich and share personal data and profiles on a large scale with an unlimited quantity of commercial businesses, without having acquired the required consent from the data subjects. This means that they do not fulfil the requirements of transparency, data minimisation and transfer either. These actions take place without the data subjects being able to exercise any control on this and often without the

[398] See also EDPB Consent, inter alia par. 36 and 104.
[399] F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming' (Compensation under the General Data Protection Regulation), MvV 2019/7.9, p. 290.
[400] P. van Schelven, 'Important points regarding GDPR liability/indemnification, can be consulted via: https://www.lrgd.nl/Portals/1/Symp_2019_materiaal/4c%20Schelven%20Aandachtspunten%20aansprakelijkheid%20en%20vrijwaring%20AVG%20en%20verwerkersovereenkomst%20-%20LRGD.pdf
[401] F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming' (Compensation under the General Data Protection Regulation), MvV 2019/7.9, p. 290; [401] P. van Schelven, 'Aandachtspunten inzake AVG aansprakelijkheid / vrijwaring', can be consulted via: https://www.lrgd.nl/Portals/1/Symp_2019_materiaal/4c%20Schelven%20Aandachtspunten%20aansprakelijkheid%20en%20vrijwaring%20AVG%20en%20verwerkersovereenkomst%20-%20LRGD.pdf.

data subjects even knowing about it. The adverse effect of these actions on Internet users is evident: their personal information is used the RTB process. Data that provide a very precise picture of personal characteristics, interests and preferences are used to influence the Internet user. Internet users suffer (a tangible form of) damage through this process, namely non-material and material damage.

a. **Non-material damage:** to date, all that has been discussed is that a breach of the GDPR results in non-material damage. The relevant case law is explained in more detail hereafter.

b. **Material damage:** although the courts, in particular, have only proceeded to reimburse non-material damage following breaches of the GDPR, such breaches can also result in material damage. This is what has happened in the case of Oracle and Salesforce too. After all, the data subjects are impacted in their property through the actions of Oracle and Salesforce. The information collected by these parties concerning the Internet users has an economic value. That this is the case follows from the sole fact that commercial parties, such as Oracle and Salesforce, are prepared to incur costs and set up a complex organisation in order to collect, or arrange for the collection of, this information. The material damage is explained in further detail in Section 0.

627. Both the non-material damage as well as the material damage should be compensated by Oracle and Salesforce. The Foundation primarily bases its claims on Article 82 GDPR and alternatively on Article 162 Book 6 of the Dutch Civil Code (wrongful act) or Article 6:212 BW (unjustified enrichment).

628. In the event of a breach of the GDPR, Article 82 GDPR gives the injured party the right to compensation for the material and non-material damage. Article 82(1) of the GDPR reads as follows:

> *"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*

5.5.2 Definition of damage under the scope of the GDPR

629. In its case law the CJEU uses the preamble as an aid to explaining the provisions of the European legislation. Recital 146 of the preamble of the GDPR states that "all damage" should be compensated and that the definition of damage should be explained in broad terms in view of the case law of the CJEU (Court of Justice of the European Union), "in a manner which does full justice to the objectives" of the GDPR.

630. As a starting point, the CJEU understands that the damage to be compensated must be real and certain. That is soon the case. In *Staelen v. Ombudsman* the Grand Chamber of the CJEU concluded that the "feeling of psychological damage" can be designated as real and certain damage.[402] In doing so, the Grand Chamber deviated from the opinion of the Advocate

[402] CJEU 04 April 2017, C-337/15, ECLI:EU:C:2017:256 (*European Ombudsman*), paragraph 127-128.

General, who was of the opinion that "*the compensation cannot only be based on the subjective statement of the party claiming that*".[403]

5.5.3 Non-material compensation

631. The definition of damage is also explained in Dutch case law in the same way. Compensation has been granted in the Netherlands several times due to violation of the GDPR. A connection is made thereby to Article 106, first paragraph, opening lines and under b, Book 6 of the Dutch Civil Code.[404]

632. On 1 April 2020 the Administrative Jurisdiction ("**Division**") gave four judgments, in which it ruled on the application for the award of compensation in connection with the processing of personal data in breach of the GDPR.[405] The Division confirms that a breach of the GDPR may under certain conditions be designated as a "violation against the person in another manner" as referred to in Article 106, first paragraph, opening lines and under b Book 6 of the Dutch Civil Code, which allows a claim for compensation for non-material damage.[406]

633. From the judgments of the Division it follows that the claim for compensation soon exists in the event of a breach of data protection law.

634. In two of the four judgments, the Division concluded that the right to data protection has not, or has only to a very limited extent, been breached.[407]

635. In a third judgment about a municipality that had mentioned a name in response to a request from other municipalities within the context of a WOB request (Freedom of Information Act), the Division comes indirectly to the same conclusion. The Division considers that it is not about "*seriously culpable behaviour with such serious consequences that it must be classified as infringement of a fundamental right*".[408] In Article 8 of the Charter, data protection law is considered as a fundamental right. In paragraph 31, the Division also refers to that provision, and in its assessment it contends first that the loss of control over personal data is a violation of personality rights.

636. In the case where the Division concludes that the data protection law *has* been violated, it grants compensation without reservation. It concerned the one-off provision of medical data by the director of the Pieter Baancentrum in disciplinary proceedings that the data subject had initiated against him.[409] The data were included in the director's defence. The disciplinary tribunal had informed the data subject. He had consequently requested the tribunal not to take the data into consideration, to which request the disciplinary tribunal listened immediately.

---

[403] Conclusion AG 27 October 2016, C-337/15 (*European Ombudsman*), marginal 114.
[404] Court of Amsterdam, 2 September 2019,ECLI:NL:RBAMS:2019:6490, (*UWV*) (civil), paragraph 18.
[405] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898; Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:899; Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:900; Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:901.
[406] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898, r.o. 36.
[407] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:900 and Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:901.
[408] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:899.
[409] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898

637. The Division considers that there is a question of acting in breach of the data protection law, and therefore the right to protection of privacy, which can be regarded a violation against the person referred to in Article 106, Book 6, paragraph 1(b) of the Dutch Civil Code.[410] The Division does not require the data subject to substantiate the non-material damage with concrete data:

> *"[t]he adverse consequences of the provision of sensitive personal data are obvious." (paragraph 36)*

638. The Division blamed the director that it concerned privacy-sensitive personal data, but considered further that the gravity and duration of the infringement are limited (Lawyer's underlining):

> *"Concerning the gravity of the infringement, the Division considers that the privacy-sensitive personal data has come into the possession of a small group of professionals and that the members of that disciplinary tribunal have a duty of confidentiality by virtue of their function. Concerning the duration of the infringement, it is important that after submitting the sensitive data on 15 January 2018, the Pieter Baancentrum took action to reverse the provision of information." (paragraph 36)*

639. Given these circumstances, the Division has awarded the data subject compensation, set equitably at an amount of € 500.[411] In the determination of the amount, the Division takes account of the nature, duration and gravity of the infringement. The appellant had taken the position that in the first instance, the court had granted too low an amount, namely € 300. The Division agreed and assigned a higher amount. The Division did not motivate why the allocation of € 500 in compensation in this case is fairer than € 300. It may be assumed that in situations where multiple factors weigh in favour of awarding compensation, this will result in a higher amount. This will be discussed in more detail in Section 0.

640. With its four judgments, the Division follows the EBI judgment of the Supreme Court of 15 March 2019.[412] In that judgment, the Supreme Court ruled that in addition to cases of mental injury, "the nature and gravity of the violation of standards and its consequences" also justify a right to non-material compensation.[413] In his *Dutch case law note* under the judgment, Lindenbergh indicates that the Supreme Court does not formulate this category as an exception to the basic principle of mental injury, but as a subordinate basis.[414]

641. That in the case of the provision of information by the director of the Pieter Baancentrum, the Division does not require the data subject to substantiate his non-material damages with concrete data, is also in line with the EBI judgment.[415] After all, in the EBI judgment, the Supreme Court ruled that where appropriate, the sufficiently adverse consequences of the violation of standards are so obvious *"that a violation against the person may be assumed*".

---

[410] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898, par. 36
[411] Administrative Jurisdiction Division 1 April 2020 ,ECLI:NL:RVS:2020:898.
[412] Supreme Court 15 March 2019, ECLI:NL:HR:2019:376 *(*EBI*)*, paragraph 4.2.1.
[413] Supreme Court 15 March 2019, ECLI:NL:HR:2019:376 *(EBI)*
[414] Supreme Court 15 March 2019, ECLI:NL:HR:2019:376 (*EBI*), NJ 2019/162 with annotation by SD. Lindenbergh, par. 11.
[415] Supreme Court 15 March 2019, ECLI:NL:HR:2019:376 *(*EBI*)*, paragraph 4.2.1.

642. The rulings make it clear that for the answer to the question as to whether a claim for damages exists, the Division puts great emphasis on the nature of the right: the right to the protection of privacy. Acting in breach of data protection law provides a "violation of personality", which justifies the claim for non-material damages. Thus, the Division does not raise the bar particularly high for the right to compensation for breaches of the GDPR.

643. This broad interpretation of Article 106 first paragraph, opening lines and under b, Book 6 of the Dutch Civil Code is also followed by the lower courts. Noord-Nederland District Court ruled on 15 January 2020 that the provision of (just) the name and address to a third party already resulted in a claim for compensation. [416] The court awarded a sum of € 250 and considered the following:

> *"The District Court is of the opinion that this involves a violation of a fundamental right, which in view of its nature and gravity means that a right to claim for compensation for that damage exists. The latter also follows from the GDPR."*
>
> *[…]*
>
> *"The sole fact that the damage cannot be described precisely and is possibly relatively small in size cannot form a ground for rejecting every claim for that." (paragraph 4.106)*

644. Amsterdam District Court came to the same conclusion in a case in which the UWV had wrongly shared special categories of personal data with a third party. [417] The UWV had mistakenly notified the new employer of the data subject that she had been ill for a long time. Although the new employer had subsequently simply extended her employment contract, the Court still awarded compensation of € 250. To that end, the Court considered the following:

> *"[T]he sole fact that the damage was (real but) relatively small in size is not [cannot form] a ground for rejecting every claim for that. An explanation in accordance with the regulation in Article 106 paragraph 1 Book 6 of the Dutch Civil Code means that [the claimant] has the right to compensation (to be determined reasonably) of her damage." (paragraph 18)*

645. A broad interpretation of the definition of damage is also maintained in other countries. The London *Court of Appeal* even ruled in *Lloyd v. Google* that loss of control over personal data was not required before separate damage was asserted and proven:[418]

> "*For the reasons, I have given, I would conclude that damages are in principle capable of being awarded for loss of control of data under article 23 and section 13, even if there is no pecuniary loss and no distress*." (paragraph 70)

646. The case concerns the collection of surf data of iPhone users by Google via Apple's web browser Safari. Contrary to the Dutch court, the English court did not refer to the national legal system

[416] Noord-Holland District Court, 15 January 2020, ECLI:NL:RBNNE:2020:247 (*NDC Mediagroep*).
[417] Amsterdam District Court 2 September 2019, ECLI:NL:RBAMS:2019:6490 *(UWV*)
[418] Court of Appeal 2 October 2019, EWCA Civ 1599 (*Lloyd v Google*).

for the award of compensation. The English court considers there to be an independent ground for a claim for compensation in Article 82 GDPR.

5.5.4 Calculation of the level of non-material compensation

647. The level of the compensation is determined in part by the objectives of the right to compensation in the GDPR. It follows from recital 146 of the GDPR that data subjects should receive a full and actual compensation. In addition, it follows from Article 84 GDPR that sanctions must be *"effective, proportionate and dissuasive"*.[419] That is a qualification that is used frequently in Union Legislation (see for example Directive 2004/48 and Directive 2006/54). The CJEU determined in the *Manfredi* ruling that the awarding of non-compensatory compensation is possible, to the extent that the principle of efficacy and the principle of equality are taken into consideration.[420]

648. When compensation (also) has the aim of the protection of data protection law in general, that means that account should also be taken of the punitive effects of such compensation. Hartlief also emphasised in his conclusion in the aforementioned EBI judgment that the enforcement of rights and obligations is one of the functions of compensation law. Especially when there is no demonstrable non-material damage, or this is difficult to demonstrate, the sanctioning of rights and obligations can play an important role in determining compensation, according to Hartlief.[421]

5.5.4.1 Relevant factors for the level of non-material compensation

649. When assessing the level of the non-material compensation, the courts maintain different factors. The general rule thereby appears to be that a weighing up of multiple factors to the advantage of an award of compensation will result in the award of a larger amount.

650. The Administrative Jurisdiction Division and lower courts have applied the following factors when assessing the level of the compensation:

a. **Nature of the data**: the Administrative Jurisdiction Division took into account the exceptional sensitivity of the nature of the personal data which were processed without the permission of the data subject.[422]

b. **Gravity of the violation/number of recipients**: the Administrative Jurisdiction Division considers it relevant that the privacy-sensitive personal data were passed on to a small group of professionals.[423]

c. **Duration of the violation:** the Administrative Jurisdiction Division considered it relevant that the controller should have immediately taken action in order to reverse the provision of data.[424]

[419] Cf. also recitals 151 and 152 of the GDPR.
[420] CJEU 13 July 2006, C-295/04 - 298/04 *(Manfredi)*.
[421] Conclusion Advocate-General Hartlief 16 October 2018, ECLI:NL:PHR:2018:1295, par. 4.4.
[422] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898, par. 36.
[423] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898, par. 36.
[424] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898, par. 36.

d. **Number of data subjects:** Noord-Nederland District Court considered it relevant that the loss of control over personal data is limited to one person only.[425]

e. **Irreversible damage:** Noord-Nederland and Amsterdam District Courts considered it relevant that the loss of control of the data subjects over the personal data was permanent.[426]

651. Insofar as a connection should be sought with Article 106 Book 6 of the Dutch Civil Code in respect of the establishment of the scale of the compensation, it holds that account must also be taken of all of the circumstances of the case. Besides the aforementioned factors, account may be taken, for example, of:

a. the **degree of culpability**; and

b. the **economic relationships** between both parties.[427]

652. In this way, a compensation amount will be larger if there is serious negligence and/or if there is an economically unequal relationship between (large-scale or other) professional market parties on the one hand and Internet users (consumers) on the other.

653. The aforementioned factors fit in with the grouping of the categories of fines in the GDPR (Article 83 paragraphs 4 and 5 GDPR) and the policy rules of the Data Protection Authority.[428] The Data Protection Authority chose a system whereby the fine has been made dependent on the severity and gravity of the violated standard and the relationship with other standards in data protection law:

a. High fines apply, inter alia, to breaches relating to sensitive personal data, the rights of data subjects and the (forbidden) transfer of personal data to third countries.

b. Lower fines will be handed down for the violation of formal obligations, such as entering into a processing agreement and the keeping of a register of personal data.

654. When establishing the level of the fine, the Data Protection Authority also takes other factors into account, such as the duration of the offence, the number of data subjects and the scale of the damage.

5.5.4.2 Flat-rate amounts /setting a price for damages

655. In this case, the Foundation is applying for the awarding of a flat-rate amount of € 500 in compensation per Claimant. Although this is not being explicitly considered, it seems that the Division and courts in the GDPR case law cited above have awarded a fixed compensation for damages.

656. In principle, a fixed compensation for damages is not consistent with the basic principle of Dutch compensation law: the actual damages must be compensated fully and estimated

[425] Noord-Nederland 15 January 2020, ECLI:NL:RBNNE:2020:247, par. 4.107.
[426] Amsterdam 2 September 2019, ECLI:NL:RBAMS:2019:6490, par. 18.
[427] TM and EV I, Dutch Parliamentary History, BW Book 6, respectively pages 377 and 388.
[428] See the Policy Rules of the Data Protection Authority of 19 February 2019 regarding the determination of the amount of administrative fines (Policy Rules of the Data Protection Authority, 2019).

concretely, with due observance of all the circumstances of the case.[429] However, exceptions are allowed in legal precedents, both for practical reasons and for reasons of equity.[430] The Foundation will explain below that in the present case too, this basic principle should be deviated from and a fixed compensation is appropriate.

657. In the proceedings on the Groningen earthquake damage, two plaintiffs claim (inter alia) a condemnation of (inter alia) the NAM and the State for non-material damages. In these proceedings, the Noord-Nederland District Court[431] referred preliminary questions to the Supreme Court, including the question as to whether the compensation could be set as fixed. The Supreme Court formulated this question as follows:[432]

> *"With preliminary question 9c, the court wishes to ascertain the extent to which the highly personal nature of non-material damages is compatible with the more or less 'fixed' setting of compensation."*

658. Regarding this question, the Supreme Court considered as follows (Lawyer's underlining):

> *"The extent of an obligation to compensate damages resulting from a violation against the person in another manner, cannot be set "more or less fixed', as that is not compatible with the highly personal nature of the claim for compensation for these damages.[433] <u>That does not affect the fact that the court may rule that the nature and gravity of the event establishing liability mean that the adverse effects relevant in this context [...] are so obvious, that it can be assumed to be a violation against the person and that in addition, the court may deem it plausible that due to this violation against the person, the damages suffered [...] amount to at least a certain amount</u>."[434]*

659. The Supreme Court thus gives a hint that under [certain] circumstances, compensation may amount to at least a certain amount: a minimum 'fixed' amount.

660. Such a minimum 'fixed amount' can be awarded if, having regard to the nature and gravity of the 'event establishing liability', its adverse consequences are obvious.

661. In the present case too, the adverse effects are so obvious that a violation against the person can be assumed and the damages should amount to at least a certain amount per Claimant. Oracle and Salesforce process large amounts of sensitive data of the Claimants on a large-scale, in the long-term, and for commercial reasons. In addition, they violate, inter alia, the GDPR and Article 11.7a of the Telecommunications Act, the right to protection of privacy, the right to privacy[435] and the data protection law[436] (nature and gravity of the 'event establishing

[429] Supreme Court 05 December 2008, ECLI:NL:HR:2008:BE9998 par. 3.3.
[430] J. Spier, *Commitments from the law and compensation* (Study series Civil law part 5), Deventer: Kluwer 2015, par. 208.
[431] Noord-Nederland 10 October 2018, ECLI:NL:RBNNE:2018:4009.
[432] Supreme Court 19 July 2019, ECLI:NL:HR:2019:1278 par. 2.13.1.
[433] ECHR 10 February 2011, no. 30499/03 (*Dubetska et.al./Ukraine*), par. 105.
[434] Supreme Court 19 July 2019, ECLI:NL:HR:2019:1278 par. 2.13.7.
[435] Article 7 of the Charter.
[436] Article 8 of the Charter and the GDPR.

liability'). There are massive, prolonged and serious infringements of fundamental rights,[437] whose harmful effects can be imagined.

662. In his note to the EBI judgment[438], Lindenbergh emphasised that in the violation of fundamental rights, it is even more obvious to connect the extent of the compensation to the nature and gravity of the violation of standards. Depending on the type of case, the pricing of claims can be used, where it is obvious to grant the same amount of damages to all injured parties. Lindenbergh gives as an example, the massive invasion of the privacy of a data breach of important private data:[439]

> *"With — in short — the violation of fundamental rights, it is, however, much more obvious to relate the extent of the compensation to the nature and gravity of the violation of standards. After all, in this respect, it rather concerns presumed consequences. That also allows, depending on the type of case, fairly good pricing (category amounts) of amounts: in a massive invasion of privacy by a data breach of important private information, it is obvious to award all injured parties the same amount".*

663. The Foundation takes the view that even in this case, it is obvious to apply to such pricing. The Claimants should be awarded one and the same minimum compensation.

664. Also for practical reasons, a fixed calculation of damages should be used. After all, massive violations of fundamental rights are involved. The settlement of such (mass) damages is promoted by applying a fixed calculation of damages. In the explanatory memorandum to the new Settlement of Mass Damages Claims in Collective Proceedings Act (WAMCA), it is noted in this respect that the use of a subdivision in fixed category (amounts) ensures that the mass damages can be settled collectively.[440] By working as much as possible with categories[441], it is as it were abstracted from individual cases. For efficient and effective mass damages arrangement, it is thus inevitable to abstract from individual circumstances.[442]

665. In addition, Article 97, Book 6 of the Dutch Civil Code stipulates that the court estimate the damages in the manner that is most consistent with its nature. This creates room to estimate the damages on the basis of pricing / damages categories.[443]

666. In view of the foregoing, in this case the Foundation is applying for the awarding of a flat-rate amount in compensation per Claimant.

---

[437] The violation of a fundamental right does not appear to be a separate criterion, as the Supreme Court speaks of an 'event establishing liability'. Otherwise: conclusion A-G Hartlief, ECLI:NL:PHR:2018:1295, par. 5.4 and further, but he is not followed in this by the Supreme Court. In the literature, it is sometimes argued otherwise. On this, see: Janssen and Bloo-Kroes, 'The jurisprudential developments of non-material damages in an exceptional violation of standards', *MvV* 2019, number 10.
[438] Supreme Court 15 March 2019, ECLI:NL:HR:2019:376 (*EBI*), *NJ* 2019/162 with annotation by SD. Lindenbergh, par. 18.
[439] Supreme Court 15 March 2019, ECLI:NL: HR:2019:376 (*EBI*), *NJ* 2019/162 with annotation by SD. Lindenbergh, par. 18.
[440] Parliamentary Papers II, session 2016–2017, 34 608, no. 3 5 pages 5 and 6.
[441] Parliamentary Papers II, session 2016-2017, 34 608, no. 3 5, page 52.
[442] T. Hartlief, Massaschade en de regelende rechter (Mass damages and the controlling court), Blog NJB 13 November 2017.
[443] Parliamentary Papers II, session 2016-2017, 34 608, no. 3 5, page 52.

5.5.4.3 Application to the present case

667. The Foundation is of the opinion that the damage suffered by the people that the Foundation is representing lends itself to a flat-rate amount, based on the factors formulated by the Division and lower courts (see Section 0):

a. **Nature of the data**: Oracle and Salesforce are processing large volumes of personal data per data subject. This data is used to create profiles of the Internet user that are deployed on a large scale for the personalisation of advertisements. These profiles contain information such as gender, town/city of residence, age, number of devices in use etc., as well as more sensitive information that includes past and present Internet searches, the websites someone visits and has visited, the articles that someone reads and has read and his/her buying behaviour. This data can be used to derive preferences and interests. What is certain is that the collected data provides a very detailed and intrusive picture about the lives of the data subjects. This makes the data sensitive by nature, unlike in the case of just a name and address for example. Moreover, it is inherent in the practices of Oracle and Salesforce that special categories of personal data are processed.

b. **Gravity of the violation/number of recipients**: Oracle and Salesforce are grossly infringing the GDPR. They share the completed profiles (which include information that is more sensitive) solely for commercial gain. The existence of profiling means that the infringement must be considered as being particularly serious and that there is an increased risk to the rights of the data subjects. The same applies to the amount of data being processed. All this is also apparent from recital 75 GDPR. Moreover, Oracle and Salesforce do not violate just one provision of the GDPR and TA, but a plurality. This processing of personal data takes place without Oracle or Salesforce having a valid basis to do so. In doing so, they also violate the fundamental principles of transparency and data minimisation and the ban on transferring data. Unlike the aforementioned rulings, where the data were shared with only one or a few parties, Oracle and Salesforce share the personal data with a very large and indefinite group of recipients, possibly thousands of parties per auction.

c. **Duration of the violation:** Oracle and Salesforce have been violating the GDPR right from its application. The violations are still taking place at the current time and will continue unless action is taken. In contrast to the aforementioned rulings, in which the violation was in each case of short duration, in this case the violation is continuous and ongoing.

d. **Number of data subjects:** the violations are industrial in scope and affect every Internet user, wherever they are in the world and in any case if they are in the Netherlands. Research shows that the cookies of Oracle and Salesforce are placed via a large proportion of the Netherlands' most popular websites (see **Exhibit 16** and Section 3.3.1). It is very probable that each Dutch resident who regularly uses the Internet has visited these websites at some time.

e. **Irreversibility of the damage:** Oracle and Salesforce have (unlawfully) disclosed personal data to third parties, which means the loss of control over the personal data is permanent. After all, it is no longer possible to find out in whose hands personal data has ended up, since the data has been traded and on-traded between hundreds of parties whose identity the Foundation (and probably Oracle and Salesforce too) do not know. It must be presumed that this information will remain available to commercial parties for ever. This means that the damage has become irreversible. An aggravating circumstance is furthermore that Oracle and Salesforce have passed on the personal data to the United States, a country that cannot be said to offer an appropriate level of protection (see in this regard Section 0).

668. The Foundation is accordingly of the opinion that, given the circumstances of this case and just like in the case of the recent ruling by the Division, [444] a flat-rate compensation amount of at least € 500 per data subject is reasonable. In comparison with the case where the Division found that amount was appropriate, in this case it concerns much more serious violations and consequences. The Division found an amount of € 500 to be fair, while it concerned just one person, a limited amount of personal data, shared in the closed circle of disciplinary proceedings, for a short period, where immediate measures were taken to safeguard the data subject's rights.

669. This holds all the more because - by virtue of Article 6:106 Dutch Civil Code – all circumstances in the case must be looked at, including the economic relationships.[445] A key issue in the case in question is that Oracle and Salesforce – two listed tech giants – have consistently processed personal data unlawfully and have enjoyed very considerable profits for years now at the expense of consumers, namely Dutch Internet users. These Internet users scarcely have any way to act against the unlawful behaviour of the Defendants. This too must be taken into consideration in the judgment.

670. Compensation of (at least) an amount of € 500 likewise appears to be right if the categories of fines of the Data Protection Authority are looked at (see marginal 653 above). The violations referred to in this writ belong in the top category of fines, since they partly relate to sensitive personal data and its transfer.

671. In comparison with the United States too – the homeland of Oracle and Salesforce – a compensation amount of (at least) € 500 is justified, as this amount lies within the range provided for by law.[446]

5.5.5 Material compensation

5.5.5.1 Introduction

672. As explained earlier, Article 82 GDPR gives a basis for non-material and material compensation caused by a breach of the GDPR.

[444] Administrative Jurisdiction Division 1 April 2020, ECLI:NL:RVS:2020:898.
[445] TM and EV I, Dutch Parliamentary History, BW Book 6, respectively pages 377 and 388.
[446] Section 11 (179.150) of the CCPA; DataGuide 2018, p. 39-40.

673. Recital 7 of the GDPR stipulates that natural persons should have control of their own personal data. Recital 85 of the GDPR further stipulates that a breach relating to personal data may result in physical, material or non-material damage to natural persons such as loss of control over their personal data.

674. The Foundation will explain below that personal data represent economic value. The Claimants have lost control of their personal data by the practices of Oracle and Salesforce. The associated economic value has been taken from them. They have thus suffered material damage. This loss must be compensated by Oracle and Salesforce.

675. The Foundation will explain in this regard that for the compensation of material damage, a connection can be made with the market value of personal data. The Foundation will also explain that it is now making a claim against Oracle and Salesforce to provide information, since not the Foundation, but Oracle and Salesforce have the relevant information available in order to estimate this market value. The Foundation will also make a request to appoint an expert who can conduct research into the market value of the personal data in the event that Oracle and Salesforce do not voluntarily hand over or provide an insight into these data.

5.5.5.2 Economic value or personal data

676. It is possible to assign a value to each of the personal data processed unlawfully by Oracle and Salesforce. After all, companies have funds to pay for the data, because the data enables them, inter alia, to provide personalised advertising on websites and thus to promote their business interests.[447]

677. The collection and processing of (personal) data has long been described as the most valuable source of income or 'the new oil'.[448] It is described as the main driver of the global economy.[449]

> *"The world's most valuable resource is no longer oil, but data."*[450]

678. Personal data represent tangible economic value. This is also confirmed in the case law in the United Kingdom and research reports in our neighbouring countries.

679. For example, the court in the United Kingdom ruled that control of personal data is a precious asset and that it is clear that personal data have economic value.[451]

> *"It is also clear that a person's BGI has economic value: for example, it can be sold. It is commonplace for EU citizens to obtain free wi-fi at an airport in exchange for providing their personal data. If they decline to do so, they have to pay for their wi-*

[447] Competition and Markets Authority, *The commercial use of consumer data, Report on the CMA's call for information*, June 2015, 61-63; United Nations, Department of Economic and Social Affairs, *Data Economy: Radical transformation or dystopia?*, Frontier Technology Quarterly.
[448] See the speech of the former EU Commissioner Kroes: http://europa.eu/rapid/pressrelease_SPEECH-12-149_en.htm.
[449] Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data, Economist (06 May 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; S.A. Elvy, *Paying for privacy and the personal data economy,* Columbia law review, October 2017, vol. 117, no. 6, p. 1371-1372.
[450] Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data, Economist (06 May 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource
[451] Court of Appeal 2 October 2019, EWCA Civ 1599 (*Lloyd v Google*).

> *fi usage. The underlying reality of this case is that Google was able to sell BGI collected from numerous individuals to advertisers who wished to target them with their advertising. That confirms that such data, and consent to its use, has an economic value. Accordingly, in my judgment, a person's control over data or over their BGI does have a value, so that the loss of that control must also have a value."*[452]

680. The Boston Consulting Group already confirmed in 2012 that the value of personal data can be equated with other means of payment and that this data is of great importance to the global economy.

> *"In an increasingly digital society, personal data has become a new form of currency."*[453]
>
> *(...)*
>
> *"From a macroeconomic perspective, it becomes clear that digital data is already a growth driver in an otherwise flagging economy."*[454]

681. Moreover the Boston Consulting Group predicted that the value created by personal data is sharply increasing every year in Europe.[455] The French institution CIGREF endorsed the findings from the report of the Boston Consulting Group.[456]

682. A research report from the Deutsches Institut für Vertrauen und Sicherheit im Internet not only confirms that personal data represents monetary value, but also points out that civil law must thus provide sufficient protection to protect this value.[457]

683. It also follows from a survey by Tim Morey, carried out among internet users, that personal data represents a monetary value. From this research, the following picture emerges with regard to the value of personal data:[458]

[452] Court of Appeal 2 October 2019, EWCA Civ 1599 (*Lloyd v Google*), r.o. 46.
[453] Boston Consulting Group, The value of our digital identity, 2012, p. 3.
[454] Boston Consulting Group, The value of our digital identity, 2012, p. 3.
[455] Boston Consulting Group, The value of our digital identity, 2012, p. 3.
[456] CIGFREF, L'économie des données personnelles, October 2015, p. 8.
[457] Deutsches Institut für Vertrauen und Sicherheit im Internet, Daten als Handelsware, 2016, p. 18, 66-67.
[458] T. Morey, What's Your Personal Data Worth?, *DESIGN MIND* (18 January 2011), https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039syour-personal-data-worth.html.

The three tiers of value

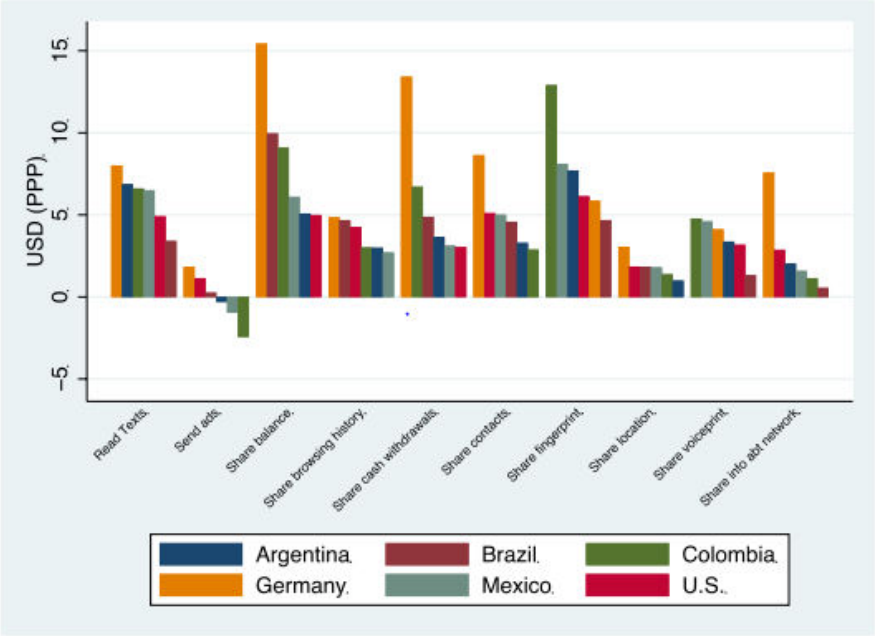
684. It can be deduced from the above overview that an individual value can be assigned to the personal data and that the value of this data may depend on the type of information. For example, the survey participants indicated that a user's citizen service number was more valuable than a user's demographics.

685. Tim Morey's survey was also cited in connection with the determination of the economic value of personal data by plaintiffs in Brown et al v Google in the United States. The Brown et al v Google case is a class action case against Google,,[459] in which Google is accused, among other things, of acting wrongfully by collecting personal data from persons using the private mode of the Chrome internet browser.

686. Recent research confirms that personal data represents monetary value, but recognises that it is difficult to determine the exact value of personal data.[460] The survey carried out by Jeffrey Prince and Scott Wallsten[461] amongst internet users in the United States, Mexico, Brazil, Colombia, Argentina and Germany, reveals the following picture regarding the different values of (personal) data:[462]

[459] Brown et al v Google LLC et al, U.S. District Court, Northern District of California, No. 20-03664, par. 70.
[460] See for instance R. Jia , What is My Data Worth?, *Berkeley Artificial Intelligence Research*, 2019; J. Prince & S. Wallsten, How Much is Privacy Worth Around the World and Across Platforms?, January 2020, *Technology Policy Institute*.
[461] Scott Wallsten is President and Senior Fellow at the Technology Policy Institute. Jeff Prince is a professor in business economics at the Kelley School of Business, Indiana University.
[462] J. Prince & S. Wallsten, How Much is Privacy Worth Around the World and Across Platforms?, January 2020, *Technology Policy Institute*, p. 6.

Figure 2: Average Payment Consumers Would Demand for Permission to Share Data to Share Data Across Countries by Feature



687. It can be deduced from the above overview that the value of personal data may not only depend on the category of data, but may also differ by country. The research also shows that the age and gender of a participant are possible factors that can also influence the determination of the value of personal data.[463]

688. Furthermore, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services confirms the economic value of data.[464] Directive (EU) 2019/770 pertains to contracts in which a trader supplies or undertakes to supply the consumer with digital content or a digital service (Article 3, paragraph 1). In return, the consumer must pay a price or provide any consideration other than money, in the form of personal information or other data.[465] This gives payment in the form of personal data a value comparable to money and the Directive (EU) 2019/770 recognises the economic value of personal data. This is also confirmed in the proposal for Directive (EU) 2019/770:

> *"In the digital economy, information about natural persons often and increasingly has a value comparable to money to market participants. Digital content is often not*

[463] J. Prince & S. Wallsten, How Much is Privacy Worth Around the World and Across Platforms?, January 2020, *Technology Policy Institute*, p. 1.
[464] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the supply of digital content and digital services, PbEU 22 May 2019. The directive entered into force on 11 June 2019 and must be transposed into national regulations by 1 July 2021 at the latest. The new rules in national law should then enter into force from 1 January 2022.
[465] *Mr. dr.* C. Spierings, *'Het nieuwe goud: betalen met data'* (The new gold, pay with data), *MvV* 2019, p. 207-214; *Mr. dr.* M.Y. Schaub, 'Nieuwe regels voor de consumentenkoop en overeenkomsten met betrekking tot digitale inhoud' (New rules for consumer purchases and digital content contracts), *NtER* 2019-9-10, p. 243-249.

provided for payment of a price, but for considerations other than money, for example in exchange for providing access to personal or other data "".[466]

689. It follows from the foregoing that personal data represents economic value.

5.5.5.3 Determination of the amount of the material damage

690. Oracle and Salesforce have collected and processed the personal data of the Victims on a large scale, for a long time and for commercial purposes. In doing so, they have, among other things, infringed the GDPR and the Tw, acted wrongfully or were unjustly enriched. The Victims have lost control of their personal data and their privacy interests have been harmed. The Victims have suffered damage (Article 6:96 of the Dutch Civil Code). The Victims can no longer control and decide on the use of their personal data. This damage must be compensated.

691. In the event that there is an obligation to pay compensation, the starting point is that full (concrete) compensation takes place (Article 6:95 of the Dutch Civil Code). In particular cases, exceptions have been accepted in case law from the starting point of a concrete damage calculation, both on practical grounds and for reasons of fairness.[467]

692. The present case concerns a special case. This concerns personal data that has been collected and processed on a large scale, long-term and for commercial purposes. The Victims have lost control of their personal data and their privacy interests have been compromised by the practices of Oracle and Salesforce. However, the damage is not easy to estimate or prove, but it has occurred frequently and on a large scale among Dutch internet users. In view of the efficient settlement of claims and fairness considerations, a rapid settlement according to objective standards is highly desirable in these circumstances.

693. When calculating the material damage, it should be taken as a starting point that personal data represent an economic value, including the personal data that Oracle and Salesforce have stolen from the Victims. The amount of the value of the loss of control over the personal data could be equated with the value that the personal data have in the normal market at large[468] or the value attributed to it in the normal market at large.

694. Oracle and Salesforce would in that case have to compensate the Victims with the (objective) market value of (the use of the) personal data.[469] The Foundation takes the position that the amount of the market value must be estimated at the value of the use of the personal data on the RTB market. This value can for example follow from the price paid by all parties on the RTB market to be allowed to use the personal data. After all, this is the price that the Victims could have negotiated for the use of their personal data from the moment that the GDPR came into force, namely 25 May 2018.

---

[466] See consideration 13 in the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, Brussels, 9 December 2015, COM (2015) 634 final, 2015/0287 (COD).
[467] Supreme Court 5 December 2008, ECLI:NL:HR:2008:BE9998, *NJ* 2009/387 (*Rijnstate/R.*); *Groene Serie Schadevergoeding* (Compensation), Section 6:98 BW, par. 4.3.
[468] Parliamentary History, BW Book 6, p. 818-819.
[469] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Unjustified enrichment and undue payment as sources of undertakings)(*Onderneming en recht* (Enterprise and law), no. 80), Deventer: Kluwer 2014, par 4.6.2 and 5.6.5.

5.5.5.4 Request for information and appointing an expert

695. The Foundation does not have this information. The (annual) figures published by Oracle and Salesforce show billions of euros in revenue, but provide insufficient insight into the revenues that are specifically generated and the mutual market prices that are applied for the use of the personal data of Dutch internet users.

696. The only way to obtain disclosure of this information is through the respective market parties. In chapter 7 "Evidence" the Foundation will set out the legal means which could be applied to obtain this information. The Foundation will also further explain in that chapter the claims for disclosure of information brought against Oracle and Salesforce.

697. Investigation by an expert into the market value of (the use of) the personal data of the Victims as of May 25, 2018, whereby Oracle and Salesforce are ordered to cooperate fully with that investigation, may provide a solution in that context. The Foundation therefore requests the court to appoint an expert pursuant to Article 194 Rv.

5.6 Liability of Oracle due to a Data breach

698. Earlier this year, a data breach occurred in connection with Oracle's DMP. This means that Oracle has not fulfilled its obligation to adequately protect the personal data it processes. This constitutes a violation of article 5 paragraph 1 under f and 32 GDPR. The incident also constitutes a breach of personal data as referred to in Article 4, paragraphs 12 and 33 and 34 of the GDPR. Oracle should therefore have reported the incident to the supervisory authority (ies) and the data subjects. It did not do this. In this connection see section 4.7.

699. It follows from recital 85 of the GDPR that a data breach may lead to material or immaterial damage. Examples of damage include: financial loss, reputational damage and loss of control of personal data.[470]

700. This damage occurred. Due to the violations, detailed information from a huge number of internet users has been disseminated. This probably also involves personal data of the Victims who are represented by the Foundation and most likely the data of an even larger group. It is certain that billions of personal data have ended up on the street. The data subjects have suffered immaterial damage, among other things as a result of the loss of control that they have suffered as a result of Oracle's actions.

701. The Foundation is of the opinion that a fixed compensation of at least €100 per data subject is reasonable for the damage caused as a result of the data breach. The Foundation also requires Oracle to provide information about the nature and cause of the data breach, as well as about its scope, the compromised data and the group of affected data subjects.

[470] These examples are also mentioned in recital 75.

5.7 In the alternative: Other grounds for liability

5.7.1 Liability on the grounds of the wrongful act

702. The Foundation bases its claims primarily on liability under the GDPR. However, the liability can also be established on the grounds of Article 6:162 of the Dutch Civil Code. In the alternative the Foundation bases its claims therefore on the wrongful act (Article 6:162 of the Dutch Civil Code).

703. Recital 146 GDPR states that the Regulation does not affect any claims for compensation for breaches of other rules in EU or national law. The option to institute a claim under Article 6: 162 of the Dutch Civil Code is thus possible in parallel with a claim under the GDPR.[471]

704. The Foundation will explain below that the basic principles of the GDPR must be taken into account when assessing its claims on the basis of the wrongful act. Therefore Article 6: 162 of the Dutch Civil Code must be interpreted in accordance with the GDPR to the extent necessary.

705. The Foundation will also explain that the requirements for a successful invocation of Article 6:162 of the Dutch Civil Code (wrongful act, attributability, relativity, causal connection and damage) have been fulfilled.

5.7.2 Article 6:162 of the Dutch Civil Code must be interpreted in accordance with the GDPR.

706. Within EU law, the doctrine of EU-compliant interpretation is important to ensure that EU law penetrates the different layers of national law. According to this doctrine, the national court and national implementing bodies are obliged to interpret the applicable national law as much as possible in such a way as to ensure compliance with the obligations arising from European law.[472] The national standard should be interpreted as far as possible in the light of the wording and purpose of the relevant European law provision in order to achieve the objectives pursued by it. The doctrine of EU-compliant interpretation applies, among other things, to directives, treaty provisions, regulations and principles.[473]

707. The Foundation takes the position that in the present case the doctrine of the EU-compliant interpretation should lead to Article 6: 162 of the Dutch Civil Code, to the extent necessary, to be interpreted in accordance with the GDPR in a way that fully does justice to the objectives of the GDPR. This means that in assessing the claims based on the wrongful act of the Foundation, the principles of the GDPR with regard to the assessment of the violations, the damage and the causal connection must be taken into account. [474]

---

[471] *Groene Serie Onrechtmatige daad* (wrongful act), par. 12.4.7.3 Ratio of Art. 82 of Regulation 2016/679 to the wrongful act. This is also confirmed by the Department in, among others, ABRvS 1 April 2020, ECLI: NL: RVS: 2020: 900, ground for decision 25 based on the implementation table for Article 82 GDPR in *Parliamentary Papers II* 2017/18, 34851 no. 3.
[472] ECJ EC April 10, 1984, 14/83 (Von Colson and Kamann), ground for decision. 26; ECJ EC November 13, 1990, C-106/89 (Marleasing), ground for decision 8; J.R. van den Brink, The implementation of European subsidy schemes in the Netherlands (R&P no. SB6) 2012 / 3.2.2.3.
[473] J.R. van den Brink, The implementation of European subsidy schemes in the Netherlands (*R&P* no. SB6) 2012 / 3.2.2.3; ECJ EC 7 January 2004, C-60/02, (Rolex), ground for decision 59; ECJ EC 13 March 2008, joined cases C-383/06-C-385/06 (ESF judgment); ECJ EC 17 January 2008, C-246/06 (Velasco Navarro), ground for decision 35; ECJ EC 5 October 1994, C-165/91 (Van Munster)
[474] M. Wissink, 2014, *The influence of EU law on national private law*, Deventer: Kluwer, p. 119 et seq.; J.R. van den Brink, The implementation of European subsidy schemes in the Netherlands (*R&P* nr. SB6) 2012/3.2.2.3.

708. In that connection the Foundation also points out a decision by the District Court of Amsterdam of 2 September 2019 on the interpretation of Article 6:106 paragraph 1 of the Dutch Civil Code (Lawyer's underlining): [475]

> *"In addition, it should be assumed that the GDPR itself formulates principles for assessing the violation, the damage and the causal connection between them. In this respect the GDPR takes as its starting point (paragraph 146 of the recital) that the concept of 'damage' must be interpreted broadly in the light of the case law of the Court of Justice, in a way that fully reflects the objectives of that regulation. Article 6: 106 paragraph 1 of the Dutch Civil Code shall be interpreted in accordance with the regulation insofar as necessary."*

5.7.3 Wrongful act, relativity and attributability

709. According to Article 6: 162 of the Dutch Civil Code, a claim for compensation requires a wrongful act. This may be an infringement of a right, an act or omission in violation of a legal obligation and an act or omission contrary to what is appropriate in society according to unwritten law.

710. In chapter 4 the Foundation explained the violations of the GDPR, the Tw and relevant fundamental rights by Oracle and Salesforce.

711. The GDPR is a European regulation. European regulations are binding in their entirety and directly applicable in all Member States (Article 288 TFEU). In accordance with Article 93 of the Constitution, directly effective provisions from European regulations can also be qualified as (equivalent to) legal obligations within the meaning of Article 6: 162 paragraph 2 of the Dutch Civil Code.[476] It follows that the violations of the GDPR by Oracle and Salesforce can be qualified as a violation of a legal obligation. This therefore constitutes a wrongful act.

712. The violation of the Tw also automatically constitutes a wrongful act now that actions were performed in violation of a legal obligation (Article 11.7a of the Tw).

713. Apart from this the actions of Oracle and Salesforce can be qualified as actions contrary to what is appropriate in society according to unwritten law. In chapter 3 the Foundation set out stating the reasons that Oracle and Salesforce play an indispensable role in the trade in personal data in connection with the RTB system, among other things by means of cookie syncing and the other actions described in section 3.2. As DMPs, they form the central data hubs in the advertising market. Oracle and Salesforce are acting in violation of a social due diligence standard by acting in this way, as a result of which the Victims have lost control of their personal data, their privacy interests have been harmed, and have suffered damage.

714. In addition, the relativity requirement should be fulfilled. The relativity requirement means that the standard to be applied must be the protection of the injured person in the violated

[475] District Court of Amsterdam, 2 September 2019,ECLI:NL:RBAMS:2019:6490, (UWV) (civiel), ground for decision 18.
[476] *Groene Serie Onrechtmatige daad* (Wrongful act), par. 5.2.3 Treaty provisions and Union law as legal obligations; A.S. Hartkamp & C.H. Sieburgh, Asser/Hartkamp & Sieburgh 6-IV 2015/16.

interest. [477] The relativity requirement is unreservedly met since Oracle and Salesforce are wrongfully processing personal data and the GDPR serves to protect the personal data of the Victims.[478]. The relativity requirement is also fulfilled unreservedly if Article 11.7a Tw is violated by Oracle and Salesforce. Article 11.7a Tw serves after all specifically to protect personal data and the privacy of users of the public telecommunication networks and telecommunication services when using cookies.[479] By not complying with the requirements of Article 11.7a Tw and placing cookies on the peripherals of internet users, Oracle and Salesforce therefore violate the specific interest that the provision seeks to protect.

715. In other words, the relativity requirement is fulfilled: all the laws violated (GDPR and Tw) by their nature serve to protect the interests of Dutch Internet users. In the event of an act contrary to what is appropriate in society according to unwritten law, the relativity requirement is already "ingrained" in the unwritten standard of care.[480] of the Dutch Civil Code.

5.7.4 Attributability

716. Next, the question must be considered whether the attributability requirement has been met. The wrongful conduct must be imputable to the perpetrator by virtue of culpability, the law or common belief.[481] The starting point of the GDPR is that in principle the extent of culpability does not matter since it is a strict liability (see section 5.3). As a result, the attributability requirement has been met now that Article 6: 162 of the Dutch Civil Code (and Article 6: 163 of the Dutch Civil Code) must be interpreted as much as possible in accordance with the GDPR.

717. Also, the attributability requirement has been met now that the GDPR violations can be attributed to Oracle and Salesforce by virtue of culpability. The actions of Oracle and Salesforce are also contrary to what is normal in society according to unwritten law, and can be attributed by virtue of culpability. After all, it is their fault that the Victims have lost control of the personal data and their privacy interests have been prejudiced.

5.7.5 Causal connection

718. Since Article 6:162 of the Dutch Civil Code (and Article 6:98 of the Dutch Civil Code) must be interpreted according to the GDPR, with regard to the wrongful act too the causal connection (CSQN connection) is already assumed (see section 5.3). It is widely assumed in the literature that strict liability has been chosen in the context of the GDPR: the mere fact that a processing violates the GDPR is sufficient to be held liable for the damage resulting from that violation.[482]

---

[477] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Undertakings by law and compensation) (*Studiereeks burgerlijk recht deel* 5), Deventer: Kluwer 2015, p. 29.
[478] Recital 2 GDPR.
[479] Explanatory Memorandum, *Parliamentary Documents II*, 1996/97, 25 533, no. 3, p. 4, 7 and 38-39.
[480] *Groene Serie* Wrongful act, art. 6:163 BW, par. 4.3.1; I. Giesen, *Toezicht en aansprakelijkheid* (Supervision and liability), Deventer: Kluwer 2005, p. 169; S.D. Lindenbergh, *Alles is betrekkelijk* (Everything is relative) (An inaugural lecture Rotterdam), The Hague: Boom Juridische uitgevers 2007, p. 13.
[481] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Undertakings by law and compensation) (*Studiereeks burgerlijk recht deel* 5), Deventer: Kluwer 2015, p. 25.
[482] F.C. van der Jagt-Vink, '*Schadevergoeding onder de Algemene Verordening Gegevensbescherming'*('Important points regarding GDPR liability/indemnification), *MvV* 2019/7.9, p. 290; P. van Schelven, '*Aandachtspunten inzake AVG aansprakelijkheid / vrijwaring'* (Points to consider concerning the GDPR liability/indemnity), to be consulted via: https://www.lrgd.nl/Portals/1/Symp_2019_materiaal/4c%20Schelven%20Aandachtspunten%20aansprakelijkheid%20en%20vrijwaring%20AVG%20en%20verwerkersovereenkomst%20-%20LRGD.pdf.

719. If contrary to expectation Article 6: 162 of the Dutch Civil Code (and Article 6:98 of the Dutch Civil Code) is not interpreted by Your Court in accordance with the GDPR, the Foundation takes the (alternative) position that in that case a presumption of a causal connection (CSQN connection) should be assumed between the wrongful act by Oracle and Salesforce and the damages suffered by the Victims. According to the Supreme Court[483] this applies if it concerns a violation of a standard that is intended to prevent a specific risk with regard to the occurrence of damage to another and this specific risk has materialised. In this case, there has been a violation of such (a) standard(s).

720. The main purpose of the standards included in the GDPR is to increase the protection of personal data and strengthen the rights of data subjects. The GDPR is intended to protect personal data, including preventing natural persons from losing control over their personal data and suffering damage. The same applies as indicated above for Article 11.7a Tw. However, Oracle and Salesforce have violated the standards of the GDPR and Article 11.7a Tw on a large scale and for a long time (see chapter 4).

721. As a result of these violations, the Victims lost control of their personal data and suffered damage. The specific risk, against which the standards included in the GDPR and Article 11.7a of the Tw are intended to protect, has thus materialised. In that case, it is reasonable to assume that a causal connection (CSQN connection) exists between the wrongful act of Oracle and Salesforce and the damage suffered by the Victims.

722. If the causal connection is not assumed in advance in the wrongful act, then there is equally a causal connection between the damage and the wrongful act of Oracle and Salesforce. After all, the damage suffered by the Victims, the Dutch internet users, is caused by the infringing acts of Oracle and Salesforce, or because Oracle and Salesforce acted in violation of a social due diligence standard, as formulated above.

723. Article 6:99 of the Dutch Civil Code can be applied in cases in which the following is an established fact:[484]

a. the person being held liable is liable for an event that may have caused the entire damage to the injured party;

b. one or more others are also liable for events that may have caused the damage of the injured party in whole or in part; and

c. the damage suffered by the injured party is the result of at least one of these events.

724. In this context, the Supreme Court held that it cannot be deduced from the requirement under c that the injured party must state - and that must become an established fact - who belongs to the circle of liable persons, because this requirement would lead to an unreasonable result.[485]

[483] Supreme Court 29 November 2002, *NJ* 2004/304 and 305.
[484] Text & Comments, Damage as a result of multiple events; alternative causality in connection with: Dutch Civil Code, Book 6, Section 99.
[485] Supreme Court 9 October 1992, ECLI:NL:HR:1992:ZC0706, *NJ* 1994/535 (*DES-dochters*).

725. Should it appear during the proceedings that other parties are jointly responsible for the damage suffered by the Victims, Oracle and Salesforce are still liable for the damage on the basis of Article 6:99 of the Dutch Civil Code. After all, in that case any party that could have caused the damage is liable.[486]

5.7.6 Damage

726. As already set out in sections 5.5.3 and 5.5.5 the Victims suffered (any form of) damage. This damage will have to be compensated by Oracle and Salesforce.

5.7.6.1 Surrender of profit (Article 104 Book 6 of the Dutch Civil Code)

727. On the grounds of Article 104 Book 6 of the Dutch Civil Code, a person who (i) omitted an wrongful act and (ii) enjoyed a profit through that, may be ordered to surrender the profit or a part of it.[487] The term profit should be interpreted thereby in the broadest sense: limiting losses also falls under the same heading.[488] For the rest, the fact that (iii) the likelihood of any (form of) damage is sufficient for the application of the Article.[489]

728. However, only if the defendant can show that no damage could have been created then the application of Article 104 Book 6 of the Dutch Civil Code cannot be invoked.[490]

729. Article 104 Book 6 of the Dutch Civil Code was introduced by the legislator, among other things, with a view to being able to combat the violations of intellectual property rights and competition rights.[491] The legislator also indicated that Article 104 Book 6 of the Dutch Civil Code can also serve in cases whereby the injured party has probably suffered damage, but that damage is difficult or impossible to prove.[492]

730. The idea behind the provision is that it is considered unreasonable to leave unauthorised profit acquired at the cost of another with the acquirer, whereby the other has probably suffered damage, but that is difficult to prove due to its nature.[493] The provision does not give the right to surrender of profit, but does allow the court a discretionary authority to estimate the damage according to the amount of the profit or part thereof and thereby forms a statutory basis for a form of abstract compensation calculation, so that a concrete disadvantage does not need to be shown by the claimant in the event of uncertainty.[494]

---

[486] Text & Comments, Damage as a result of multiple events; alternative causality in connection with: Dutch Civil Code, Book 6, Section 99; T.F. Walree, '*De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens'* (The compensable damage on wrongful processing personal data), *WPNR* 25 November 2017/7172, p. 923.
[487] Compensation for the injured party is excluded, because otherwise the rectification would occur twice, the injured party would receive more than that to which he is entitled and the injuring party would receive a sanction twice, see Rotterdam District Court 17 October 2012, ECLI:NL:RBROT:2012:BY1147, legal ground 5.8.
[488] Supreme Court 18 June 2010, ECLI:NL:HR:2010:BL9662, NJ 2015, 33, legal ground 3.3.3 (Setel/AVR Holding); J. Spier Compensation: general, part 3 (Monographies New Dutch Civil Code partB36) Deventer: Kluwer 1992, no. 39.
[489] Text & Commentary of the Dutch Civil Code, Estimating damage; surrender of profit in Dutch Civil Code Book 6, Article 104 General compensation 2 (Mon. Dutch Civil Code no. B35) 2017/12.
[490] Green Series on Compensation, 2. Nature of the claim for surrender of profit and compensation demanded in: Dutch Civil Code Book 6 Article 104.
[491] Dutch Parliamentary History Invw. Book 6, p. 1266-67 (MvA II).
[492] Dutch Parliamentary History Invw. Book 6, p. 1269 (MvA II); Netherlands Supreme Court ruling dated 16 June 2006, ECLI:NL:HR:2006:AU8940, NJ 2006, 585, legal ground 3.5.2 (Kecofa/Lancôme): T. Hartlief, SRB 2015, p. 266.
[493] Answers II, Dutch Parliamentary History, Dutch Civil Code Book 6, p. 1269.
[494] Supreme Court 24 December 1993, ECLI:NL:HR:1993:ZC1202, NJ 1995/421 (W./N.), Supreme Court 24 June 2016, ECLI:NL:HR:2016:1309, NJ 2016/300 (Vitesse/Gelderland); Supreme Court 18 June 2010, NJ 2015, 32 (Stichting Ymere), legal ground 3.2.3, 3.7.

731. Furthermore, it follows from case law that the compensation to be imposed does not need to be in real proportion to the damage which the injured party has actually suffered. The damage should also be estimated on only a part of the profit if the financial advantage that the debtor achieved is substantially higher than the probable scale of the damage.[495]

732. Regarding the level of the surrender of profit, the court has a great deal of freedom. Establishing the damage is mainly a question of valuation, whereby no high demands can be set in relation to evidence[496] and substantiation[497]. It is sufficient that the existence of any type of damage is plausible.

733. Furthermore, the court may, when answering the question whether or not it will estimate the damage on the full amount of the profit, accord weight to the level of culpability.[498]

734. The Foundation does not have any information concerning the profitability of the DMP services of Oracle and Salesforce. It is true that the (annual) figures published by Oracle and Salesforce show billions of euros in income, but they do not provide an adequate insight into the revenues that are specifically generated in the Netherlands during the relevant period - the GDPR being in force (25 May 2018) up to and including the date on which the judgement is to be rendered.. One indication of the value of the income is the price paid by Oracle and Salesforce for the takeover of companies which are actively involved in the RTB system (margin numbers 50 and 52). The total sum of that amounts to more than € 5 billion. The Foundation is unable to make a distinction to what extent this value is determined by activities in the Dutch market.

735. It is the responsibility of Oracle and Salesforce, if Your Court should choose to seize the gain enjoyed by Oracle and Salesforce during the period from the date on which the GDPR became applicable, to provide clarity about that.[499] This is why the Foundation is also applying to this District Court to order Oracle and Salesforce to provide specific information that at least makes it possible to estimate the earnings and benefit they have enjoyed during the period from the GDPR becoming effective up to and including the date of the judgement in this case. For the time being, the Foundation assumes that the gain enjoyed by Oracle and Salesforce (each) in that period amounts to at least €500 per Victim.

736. Finally, the Foundation notes that it is of the opinion that Your Court may make use of its discretionary powers to estimate that the total damage can be equal to the total amount of the earnings, given the degree of culpability in respect of the conduct of Oracle and Salesforce (nature of the data, gravity of the violation, duration of the violation, number of data subjects

---

[495] Supreme Court 18 June 2010, NJ 2015, 32 (Stichting Ymere), legal ground 3.7; Supreme Court 18 June 2010, ECLI:NL:HR:2010:BL9662, *NJ 2015/33* (Setel/AVR) legal ground 3.3.2.; Green Series Compensation, 2 Nature of the claim for surrender of profit and the compensation demanded in: Dutch Civil Code Book 6, Article 104.
[496] Supreme Court 12 March 2010, ECLI:NLIHR:ZOlOZBK9ISS (X-lnterpolis and Achmea), RvdW 2010, 416, legal ground 3.4; W. Dijkshoorn & S.D. Lindenbergh, 'Estimating damage, evidence and valuation', Ars Aequi 2010, p. 541.
[497] Supreme Court 17 February 2006, ECLI:NL:PHR:2006:AU9717 (Royal & Sun Alliance/Polygram) NJ 2006, 378, legal ground 4.8; P.A. Fruytier, 'The broad approach of the Supreme Court when estimating damage in respect of profit: a step too far?', *MvV* 2010, p. 274.
[498] Text & Commentary on the Dutch Civil Code, Estimating the damage; surrender of profit in: Dutch Civil Code Book 6, Article 104 Supreme Court 18 June 2010, ECLI:NL:HR:2010:BL9662, NJ 2015/33 (Setel/AVR Holding).
[499] See for instance District Court of Amsterdam 22 January 2018, ECLI:NL:RBAMS:2018:275, grounds for decision 2 and 22; HR 14 November 2014, ECLI:NL:HR:2014:3241, grounds for decision 4.2.3 and 4.10, District Court of The Hague, ECLI:NL:RBDHA:2017:1418, ground for decision 4.1.

and irreversibility of the damage). The Foundation has gone into this point in more detail in Section 5.5.4.3 'Application to this case' above.

5.7.6.2 Abstract estimate of damage as an alternative manner of estimate of damage

737. Only in exceptional cases are exceptions made to the basic principle of the concrete estimate of damage accepted, both for practical reasons as well as reasons of fairness.[500] Article 97 Book 6 of the Dutch Civil Code forms the legal basis for the so-called abstract estimate of damage or abstract calculation of damage. The term 'abstract' means that an abstraction is made from the concrete circumstances of the case.[501]

738. In the event of an abstract estimate of damage, the circumstances of the case do not form the basis for the calculation of damage, but positions comparable to that of the injured party are reviewed. Establishment then takes place according to objective standards. Using the abstract method, the court investigates how high in general the damage is of a creditor who finds themselves in a similar position to that of the claimant in the proceedings.[502] Connecting factors for an abstract approach can be found in the nature of the damage, requirements of fitness for purpose and in the reasonableness of the result.[503]

739. The court has the freedom to do so, provided that this manner of estimation is in accord with the nature of the damage. Whether that is the case is left to the court to decide, with due regard for the aforementioned basis, of course except when the law contains a special rule on this point, which is binding for the court.[504]

740. The case in question is characterised by the fact that the Victims lost control of their personal data. Without their consent, its use, enjoyment or exploitation by Oracle and Salesforce is not permitted. However, this is actually what has happened. Oracle and Salesforce have on a large scale, for a long time and for commercial purposes, collected and processed the personal data of the Victims. Amongst other acts, they have violated the GDPR and the Tw. Victims have lost control over their personal data and have had their privacy interests harmed.

741. Oracle and Salesforce have used the personal data of Victims without their consent, without asking for their consent or paying a fee for this. In actual practice, for the time being Internet users (in this case, Victims) do not ask for any usage fee for the use of their personal data by such parties as Oracle and Salesforce. In many cases, they are not even aware that their personal data is being used and by whom.

742. The actions of Oracle and Salesforce have caused damage to the Victims. This damage cannot be easily estimated or proven. An abstract way of estimating the damage could offer a solution in this case. Given the nature of the violations (this relates to personal data and to the privacy of Dutch Internet users) and the gravity of the violations (serious long-term violation on a large

[500] J. Spier, Commitments from the law and compensation, 2015, paragraph 208
[501] A.J. Verheij, Unlawful act (Monographs Private law no. 4), 48 Estimation of damage.
[502] Asser/Sieburgh 6-II 2017/35; Text & Commentary on the Dutch Civil Code, Estimating the damage in: Dutch Civil Code Book 6, Article 97
[503] S.D. Lindenbergh, Compensation: general, part 1 (Monographs on the Dutch Civil Code B34) 2014, p. 53.
[504] Parliamentary History, Dutch Civil Code Book 6, p. 339 (Memorandum of Reply II).

scale and for commercial purposes), the Foundation takes the view that compensation of € 500 per person is fair compensation.

5.8 Unjustified enrichment

5.8.1. Introduction

743. In the further alternative, the Foundation bases its claim for compensation on unjustified enrichment (Article 212 Book 6 of the Dutch Civil Code). In the following paragraphs, four requirements for such a claim will be discussed in further detail and an explanation will be given that this is fulfilled in this case; The four requirements are (i) there is evidently enrichment; (ii) the enrichment was created at the cost of another, who was impoverished; (iii) the enrichment and the impoverishment are adequately connected to each other and (iv) the enrichment is unjustified.[505]

744. The formulation of Article 212 Book 6 of the Dutch Civil Code leaves a great deal of room for interpretation.[506] The legislator consciously chose to formulate Article 212 Book 6 of the Dutch Civil Code in abstract words in order to give the claim a wide scope of application.[507] With the choice of a general, abstractly formulated provision, the legislator has left it to the judicial system and the literature to outline Article 212 Book 6 of the Dutch Civil Code and to provide further details to the requirements of this Article.[508] A statutory framework will be sketched out per requirement according to the literature and the judicial system, after which this will be applied to the case.

5.8.2 Enrichment

745. Firstly, for the compensation of damage pursuant to Article 212 Book 6 of the Dutch Civil Code, the existence of an enrichment, is required. The term enrichment comprises both a gain achieved as well as a loss averted.[509] Enrichments come in a variety of forms and should be interpreted broadly.[510]

746. Enrichments involve a 'shift of assets'.[511] Linssen argues that Article 6:212 BW also applies if a debtor violates a legal position of another that deserves protection. His arguments are in line with the German law on enrichment and tort.[512] In the literature the ideas of Linssen are quoted, discussed and further detailed in various places.

747. Damminga broadly agrees with Linssen's view that a claim based on Article 6: 212 of the Dutch Civil Code arises in cases in which the debtor has infringed an exclusive legal position without

---

[505] *S. R. Damminga, Unjustified enrichment and undue payment as sources of commitments (Onderneming en Recht guide nr. 80), Deventer: Kluwer 2014/paragraph 1.1.1.*
[506] *S. R. Damminga, Unjustified enrichment and undue payment as sources of commitments (Onderneming en Recht guide nr. 80), Deventer: Kluwer 2014/paragraph 1.1.1.*
[507] Dutch Parliamentary History, BW Book 6, p. 829.
[508] Dutch Parliamentary History, BW Book 6, p. 831.
[509] *Groene Serie* Law of obligations, Article 212 Book 6 of the Dutch Civil Code, note 4.2.1; See Supreme Court 24 May 2013, ECLI:NL:HR:2013:BZ1782, NJ 2013/540 (Credit Suisse/SuBWay Rotterdam).
[510] *Groene Serie* Law of obligations, Article 212 Book 6 of the Dutch Civil Code, note 4.2.3.
[511] Dutch parliamentary History, BW Book 6 p.832: A.S. Hartkamp & C.H. Sieburgh: mr. C. Assers' manual for the practising of Dutch Civil Law, 6-*Law of commitments, Part* IV, *Commitments from the law, Deventer: Kluwer 2011, nr. /465.*
[512] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing* (Surrendering a benefit and unjustified enrichment: a comparative law consideration) The Hague, BJu 2001, p. 472.

causing concrete damage. He takes the position that Article 6: 212 of the Dutch Civil Code should be limited to cases in which the debtor has infringed an exclusive legal position.[513]

748. According to Linssen, this relates to a violation of the debtor's legal position, from which legal position it follows that the entitled party /debtor is exclusively authorised to use, exploit and dispose of the legal position.[514] An example of such legal positions are personality rights but other categories are conceivable too. Only the entitled party is authorised to decide over these personality rights and that person alone is entitled to the use, the enjoyment and exploitation of the gains which can be achieved from those. When another person has made use of those, this concerns a violation of the legal status of the entitled party.[515]

749. Only if the action may solely be carried out in the legal relationship between the creditor and debtor exclusively by the creditor, may it be said that the carrying out of the unauthorised action by the debtor forms a gain, which arises from the assets of the creditor.

750. Linssen gives the following example: suppose A owns a holiday home. Therefore, according to article 5: 1 of the Dutch Civil Code, he is the only one who can enjoy and use the house. If B makes use of A's property, for example by moving into A's holiday home, B obtains a benefit at the expense of A; the use itself constitutes the benefit. According to Linssen, it should be irrelevant whether A lost income due to the use by B, suffered other damage, or whether B 's assets increased or whether B saved himself costs through use. The benefit that B enjoyed at the expense of A must, according to Linssen, be equated with a reasonable user fee.[516]

751. According to Linssen, the question whether a benefit is a consequence of a particular exclusive legal position depends on the facts and circumstances of the case, including the nature of the property right and the nature of the benefit. Linssen notes that the weighting of the facts and circumstances is of course also coloured by social developments. Linssen then lists six groups of cases as an infringement of an exclusive legal position, but indicates that the list is not intended to be exhaustive:[517]

(i) Unauthorised possession and use of other people's property;

(ii) Using and exploiting secret information;

(iii) Violation of rights relating to personality;

(iv) Infringement of contractual relationships by a third party;

(iv) Breach of contractual relationships by a contract party; and

(vi) Abuse or inappropriate use of relationships of trust.

---

[513] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (*Unjustified enrichment and undue payment as sources of commitments*) (O&R nr. 80) 2014, par. 4.2.5 and 4.4.6.
[514] *J.G.A. Linssen, Surrendering a benefit and unjustified enrichment: a comparative-law consideration, The Hague, Boom Legal Publishers 2001, pp.427-473*
[515] *S. R. Damminga, Unjustified enrichment and undue payment as sources of commitments (Onderneming en Recht guide no. 80), Deventer: Kluwer 2014,para. 4.4.6.*
[516] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing (Unjustified enrichment and undue payment as sources of commitments)*, The Hague: Boom Juridische uitgevers 2001, p. 589-591.
[517] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing (Unjustified enrichment and undue payment as sources of commitments)*, The Hague: Boom Juridische uitgevers 2001, p. 586 e.v.

752. Linssen appears to be starting from the claim for unjustified enrichment as an instrument of "property protection", an extension of the "ownership right". The doctrine of unjustified enrichment is then applied to infringements of property and comparable financial positions.

753. The Foundation takes the position that the doctrine of unjustified enrichment also applies to the unlawful use of personal data by Oracle and Salesforce. Where necessary, the Foundation will add nuances to Linssen's view.

754. Firstly, the Foundation notes that, strictly speaking, personal data does not (at the moment) qualify as "property" within the meaning of Article 5: 1 BW, but that the last word has not yet been said or written about this. During a debate in the Lower House on 10 September 2019, questions were asked about the possibility of regulating in the Civil Code the citizen's ownership of his or her personal data with the government.[518] This was done in response to an advisory report on the effects of digitisation for the constitutional relations of the Council of State.[519] Mr. Van Der Molen said (on behalf of the CDA) the following during this debate:

> *"As far as we are concerned, every Dutch person should be the owner of his or her personal data or data. (...) In our opinion, an unambiguous legal provision should provide citizens with certainty and a solid basis for the relationship of the data to government platforms, among other things."*

755. The State Secretary for the Interior and Kingdom Relations promised to conduct further research or have this conducted into the possibilities of regulating the ownership of personal data. On 15 June 2020, the Lower House was informed of the outcome of this research. But the letter to the Lower House shows that the State Secretary for the Interior and Kingdom Relations is of the opinion that unlimited control over personal data is not (yet) an issue, [520] but this does not alter the fact that there is a public debate in full swing about the protection and status of personal data.

756. Second, the Foundation notes that personal data must enjoy the protection of Article 1 First Protocol ECHR ("**Protocol**"). There are three main rules contained in Article 1 of the Protocol: (i) the principle of undisturbed enjoyment of property (first sentence of paragraph 1), (ii) protection against deprivation of property (second sentence of paragraph 1), and (iii) the possibility of regulation of ownership (second paragraph).[521]

757. Property within the meaning of article 1 of the Protocol does not have the meaning that the term in article 5: 1 of the Dutch Civil Code has. The European Court of Human Rights assigns to the concept an entirely autonomous meaning, which is many times broader than the concept of ownership in Article 5: 1 of the Dutch Civil Code.[522]

---

[518] *Parliamentary Documents II*, 2018/19, 26 643, no. 105.
[519] Unsolicited advice on the effects of digitisation for the constitutional relations of the Council of State of 31 August 2018, *Parliamentary Documents II*, 2017/18, 26 643, no. 557.
[520] *Parliamentary Documents II,* 2019/20, 32 761, no. 165.
[521] ECHR 23 September 1982, NJ 1988/920 with annotation by Alkema (Sporrong & Lönnroth/Zweden), ground for decision 61).
[522] D.G.J. Sanderink, The ECHR and substantive environmental law (State and Law no. 22), Deventer: Wolters Kluwer 2015, par. 2.6.2.

758. The limits of the protection under Article 1 of the Protocol are derived from the basic idea: the protection of (economic) interests that are sufficiently certain, or in other words: form part of the assets of the relevant protected person with sufficient certainty. [523] Central to this is the protection of someone's actual assets, at least of the components that represent a concrete and certain economic value.

759. Personal data forms part of an individual's assets and represents a concrete and certain economic value (see section 5.5.5.2 above). Personal data must thus enjoy the protection of Article 1 of the Protocol and following on from this: the protection of the claim based on unjustified enrichment.

760. Third, the Foundation notes that a claim based on unjustified enrichment should not be limited to an instrument of "property protection". There is a chance that equal cases will be treated unequally. In the cases listed by Linssen, an enrichment claim would succeed when it comes to intellectual property rights, corporate opportunities and confidentiality obligations, but not, for example, when it comes to improperly taking advantage of breach of contract. And it is precisely in that case that it may be suitable for a claim based on unjustified enrichment to be used.

761. The legislator has left the development of the claim based on unjustified enrichment to case law and literature. In the judgment of the Supreme Court [524] on a Ponzi Scheme that was committed, the claim based on unjustified enrichment was used in a fraud case (taking advantage of a breach of contract). The ruling confirmed that enrichment of a party to an agreement at the expense of a third party is not always and simply justified by that agreement, even though it will usually be the case. [525] However, if there is a disparity between the performances required by the agreement on the one hand and the enrichment on the other, the agreement will less likely be accepted as a justification for the enrichment. So the claim based on unjustified enrichment also offered a solution since this Ponzi Scheme obviously entailed a disparity.

762. Fourth, the Foundation takes the position that, strictly speaking, personal data may not be property, but that the protection of personal data is related to rights relating to personality, as we know them, for example, in copyright law. Just like removing the name or modification of a copyright-protected work without permission, the use without grounds (such as consent) or otherwise wrongful use of personal data also leads to liability. With the GDPR, the European legislator wanted to enable the data subject to exercise control over the protection of personal data. By acting in violation of the GDPR, Oracle and Salesforce infringe the exclusive legal position of the data subjects.

763. Linssen notes that the "exclusive authority" of the entitled party does not always have to be absolute. Linssen states that the unauthorised use and exploitation of secret information is reserved for those who have collected or developed this information in the course of his profession or business. The exclusivity of being entitled to the information may be relative because certain persons are not allowed to use, exploit or dispose of the information while

[523] J.M. Emaus, 'Protection of goodwill under the ECHR', NTBR 2018/8, par. 3.1.
[524] Supreme Court 28 October 2011, ECLI:NL:HR:2011:BQ5986, *NJ* 2012/496 (*Ponzi-scheme*).
[525] Supreme Court 20 September 2002, ECLI:NL:HR:2002:AE3363, *NJ* 2004/458 with annotation by Hijman (*Carribean Bistros c.s. Club/Caraibeen*).

certain third parties are allowed to, for example because they have been licensed. If the person who is not allowed to use the information nevertheless does so, then he would have to hand over the benefit received thereby to the person towards whom he was obliged to refrain from using it.

764. The data subject is exclusively entitled with regard to his personal data to monitor the processing and to enforce his rights. Without observing the GDPR, his personal data may not be collected, used and/or exploited. And that is what happened in the present case.

765. Oracle and Salesforce have unlawfully collected, used and exploited the personal data of the Victims. The Foundation takes the position that Oracle and Salesforce must surrender the benefit they enjoyed due to this on the basis of unjustified enrichment. Oracle and Salesforce have enjoyed a benefit (enrichment) that arises from the assets of the Victims.

766. This act of enrichment has to give rise to a certain enrichment that can be estimated to be a certain amount. This enrichment (or 'damage') must be surrendered by virtue of Article 6:212 BW. The Foundation argues that the scale of the enrichment must be estimated over the value which the use, enjoyment or exploitation of the personal data has in legal transactions. This value may be calculated, for example, from the compensation which the Victims could have demanded.[526] The Foundation is of the opinion that this compensation can be set at an amount of € 500 per Victim.

767. In section 5.1 the Foundation explained with reasoning that it finds a compensation payment of € 500 per data subject to be reasonable, given the circumstances of the case in question. In this context, the Foundation notes that damages can be calculated in an extrapolated way, in order to ensure that Oracle and Salesforce are not allowed to keep the benefit that they have unlawfully enjoyed.

5.8.3 Impoverishment

768. There is a case of impoverishment both by a decrease in the assets as well as an increase in the liabilities.[527] The enrichment is not required to be the mirror image of the impoverishment.[528] An item of property which enriches one person at the expense of the other can have a completely different value for both of them.[529] For a collector, for example, a missing example will generally have a greater value than for the person who simply owns the example. Also when someone wishes to install a swimming pool in their garden and need a small piece of land from the neighbour, they will place far more value to that than the neighbour, if the small piece of land forms a relatively meaningless part of the neighbour's grounds.[530]

---

[526] *S. R. Damminga, Unjustified enrichment and undue payment as sources of commitments (Onderneming en Recht guide nr. 80), Deventer: Kluwer 2014/para. 4.6.2; Dutch Parliamentary History, BW Book 6 pp. 818-819*
[527] *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraph 312; *Groene Serie* Law of obligations, Article 212 Book 6 of the Dutch Civil Code, note 4.1.2.
[528] R. Koolhoven, *Dutch Enrichment Law*, Göttingen: V&R unipress 2011, p. 67; A.S. Hartkamp & C.H. Sieburgh, mr. C. Assers' manual for the practising of Dutch Civil Law, 6-*Law of commitments, Part* IV, *Commitments from the law, Deventer: Kluwer 2011, nr. /461.*
[529] *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraph 312.
[530] *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraph 312..

769. It is generally asserted that the impoverishment determines the maximum of the compensation which must be paid by the enriched person. This statement has met with much criticism in the literature. Particularly under the scope of parties who have suffered no damage or of which it is difficult to demonstrate the impoverishment, while the enriched person has, however, enjoyed a substantial gain from a violation of personality rights, for example. Therefore, at the core, this concerns the question why the unjustified person may keep his gain in those cases, while that gain actually belongs to the impoverished person.[531] It should not be necessary in those cases to be required to demonstrate (the scale of) the impoverishment.

770. In this context, it may be stated that unjustified enrichment is actually not a ground for compensation, but for a reversal of the enrichment, according to the literature.[532] This is also confirmed in the parliamentary history. It is clear from the parliamentary history that the legislator wanted to implement a general claim for surrender of an unjustified enrichment in order to fit in with the legal systems in the countries surrounding the Netherlands, as well as the early national law.[533] In those legal systems, the claim covers the surrender of the enrichment.

771. However, it appears that on the implementation of the law the legislator formulated the claim concerning unjustified enrichment as a compensation claim, contrary to what is the case in our surrounding countries. The claim appears to cover the compensation of the damage of the impoverished person, so that, for example, part 6.1.10 (Articles 95-110 Book 6 of the Dutch Civil Code) concerning legal obligations for compensation seem to apply.

772. Various problems are mentioned in the literature, which arise when the claim concerning unjustified enrichment is interpreted as a compensation claim. For example, Article 98 Book 6 of the Dutch Civil Code determines that compensation is only eligible for the damage which is connected in such a way with the event on which the liability rests, that it can be attributed to the person who is obliged to compensate as a result of this event. However, the liability involved in the unjustified enrichment rests on a situation, the enrichment, and not on an event. Even the arrangement concerning own fault contained in Article 101 Book 6 of the Dutch Civil Code assumes liability arising as a result of an event. Both Articles should not be applied to a claim concerning unjustified enrichment. Article 212 Book 6 of the Dutch Civil Code contains does, however, contain its own rule of causal connection, namely the rule that the enrichment was acquired 'at the expense of' another person.[534]

773. It is argued in the literature that if the impoverished party has not suffered any damage or if he finds it difficult to prove the damage then a claim for the surrendering of the benefit may be instituted by virtue of Article 6:212 BW instead of a claim for compensation. The words 'at

---

[531] J. *Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraph 312; *J.G.A. Linssen, Surrendering a benefit and unjustified enrichment: a comparative-law consideration , The Hague, Boom Legal Publishers 2001, p.453 ff.; S. R. Damminga, 2014, Unjustified enrichment and undue payment as sources of commitments (Onderneming en Recht guide nr. 80),* p. 202 ff.; Van Boom, pre-advice VBR 2002, paragraph 2; Hartkamp 2001, p. 315.

[532] A.S. Hartkamp, *Unjustified enrichment as well as agreement and unlawful act*, WPNR 2001/6440-6441, p. 315; B.W.M. Nieskens-Isphording, The fait accompli in property law, Deventer:Kluwer 1991, pp. 67-68; J.G.A. Linssen *Surrendering a benefit and unjustified enrichment: a comparative-law consideration , The Hague, Boom Legal Publishers 2001,* pp. 473-494; M.H. Bregstein *Unjustified increase in assets, Amsterdam: H.J. Paris* 1927, p. 216; H.C.F. Schoordijk *Unjustified increase in assets*, Zwolle: W.E.J. Tjeenk Willink 1977, p. 32; W. Snijders 2001, p. 17.

[533] Dutch Parliamentary History, BW Book 6, pp. 823-829.

[534] A.S. Hartkamp, *Unjustified enrichment as well as agreement and unlawful act*, WPNR 2001/6440-6441, p. 315

the expense of another' and 'to reimburse his loss' then solely serve to establish which person can institute the claim for unjustified enrichment. The requirement of impoverishment is then fulfilled if the benefit arises from the assets of the enrichment creditor[535] This solution is then justified by the fact that the enriched person has indeed enjoyed benefit and if it cannot be recognised why the unjustified enriched person should be able to retain that benefit.[536]

774. In the Dutch Supreme Court's Credit Suisse/Subway ruling[537], a similar solution was found for the case where in principle the impoverished party did not appear to have suffered any damage. The Dutch Supreme Court found as follows:

> *'The case in question is characterised by the fact that Subway, as the sitting sublessee of the commercial premises, has negotiated – after the termination of the lease that its co-contracting party Easy had entered into with Credit Suisse – with the latter about the formation of a lease with Subway under which Subway could continue to use the commercial premises during the period when the negotiations were continuing, and that the negotiations were terminated without a lease being formed between the parties. Under such circumstances, in principle a usage fee is owed by virtue of Article 6:212 BW for this continued use. After all, the party that continues to use the commercial premises is enriched, because it is a generally accepted practice that as a rule, the use of another's commercial premises only takes place for a remuneration, whereas the sublessee is relieved of the obligation that was agreed with his co-contracting party to pay the rent, as the result of the termination of the subletting agreement. The owner of the commercial premises suffers damage through the continued use, even if he does need to lease replacement commercial premises elsewhere and that use does not prevent him from letting out the premises to a third party. Given the analogy with the cases that are regulated in Articles 7:225 and 7:230a BW, it comes within the framework of the law that the damage to the owner in the case in question be calculated using objective criteria. The causal link between this enrichment and the impoverishment is determined by the circumstances of the case. Finally, acceptance of an enrichment claim is not unreasonable in principle because the use of the commercial space was knowingly continued with by the user, with the resulting benefit accordingly not being imposed on him, whereas this claim is only allowable up to the lowest amount of the enrichment and impoverishment.'*

775. It is also argued in the literature that in this case, use may also be made of the phenomenon of abstract compensation. When the damage of the impoverished person is estimated, unreasonable outcomes may ensue.[538]

776. The Foundation argues that the impoverishment requirement is fulfilled since the wrongly enjoyed gain of Oracle and Salesforce arises from the property of the Victims. The Victims lost

---

[535] *S. R. Damminga, Unjustified enrichment and undue payment as sources of commitments (Onderneming en Recht guide nr. 80),* Deventer: Kluwer 2014, paragraph 4.3.3

[536] J. *Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraph 312;

[537] Netherlands Supreme Court ruling dated 24 May 2013, ECLI:NL:HR:2013:BZ1782, NJ 2013/540, JOR 2013/266, with note S.R. Damminga

[538] M.H. Bregstein *Unjustified increase in assets*, Amsterdam: H.J. Paris 1927, p. 216; H.C.F. Schoordijk *Unjustified increase in assets*, Zwolle: W.E.J. Tjeenk Willink 1977, p. 32; W. Snijders 2001, *Unjustified enrichment and payment transactions,* Deventer: Kluwer 2001, p. 17; *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, page 380..

control of their personal data. Oracle and Salesforce have caused damage. Victims are thus impoverished and have suffered 'damage' or to have the right to the surrendering of the benefit enjoyed by Oracle and Salesforce, as set out above. This means that by virtue of Article 6:212 BW, the Victims may (more in the alternative) be able to institute proceedings for a claim concerning unjustified enrichment in respect of Oracle and Salesforce for the reimbursement of damage or for the surrender of the benefit unlawfully enjoyed.

5.8.4 Existing causal connection

777. The impoverished party can only institute a claim against the party who has been enriched at his expense. A causal connection must exist between the enriching and the impoverishing, which lies in the event through which the enrichment has taken place. It is unnecessary for the causal connection concerns the impoverished person and the enriched person: the enrichment does not need to have been caused by the enriched person and/or the impoverished person. This may also have occurred through the actions of a third party. [539]

778. As explained above ,the control and enforcement of rights with regard to the collection, use and exploitation of the personal data is reserved to the Victims. The personal data form part of the assets of the Victims and represent an economic value.

779. The Foundation takes the position that the personal data must enjoy the protection of Article 1 of the Protocol or that the rights which the data subjects have with regard to their personal data must be treated equally with exclusive legal positions (such as ownership).

780. Wrongful processing of the personal data by Oracle and Salesforce therefore constitutes a shift of assets at the expense of the Victims. Oracle and Salesforce enjoyed a benefit that arises from the assets of the Victims. This provides the causal connection.

5.8.5 Unjustified enrichment

781. Whether unjustified enrichment exists depends on the circumstances of the case. The legislator provided no detailed description of the term at the time. There are, however, the necessary examples in the parliamentary history when there is or is not a case of justification.[540] Any further explanation is left to the judicial system and research.[541]

782. An enrichment is unjustified if it is not based on either a valid legal act between the impoverished person and the enriched person or a legal arrangement covering that shift of

[539] *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraph 313. See for instance Netherlands Supreme Court ruling dated 29 January 1993, ECLI:NL:HR:1993:ZC0845, NJ 1994/172, with note from P. van Schilfgaarde (Vermobo/Van Rijswijk); Netherlands Supreme Court ruling dated 27 June 1997, ECLI:NL:HR:1997:AG7249, NJ 1997/719 with note J. Hijma (Setz/Brunings); and Netherlands Supreme Court ruling dated 30 September 2005, ECLI:NL:HR:2005:AR7928,NJ 2007/154 with note J.B.M. Vranken (Koker/Cornelius).
[540] Dutch Parliamentary History, BW Book 6, pp. 829/830, 833 ff.
[541] *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, paragraphs 315/316.

assets.[542] The lack of a valid and legitimate cause for the enrichment forms the primary criterion for the unjustification.[543]

783. The control of and enforcement with regard to the wrongful use of the personal data of the Victims is reserved to the Victims.

784. It not only follows from the foregoing that the collection, use, exploitation or the exercising of control of the personal data by Oracle and Salesforce constitutes a shift of assets at the expense of the Victims, but also the exercising of control of this and the enforcement of rights in this connection do not accrue to any person other than the Victims and therefore, without justification, lead to an unjustified enrichment.

785. In addition, it also applies that no justification for the enrichment can be found in the law. Far from it: Oracle and Salesforce are guilty among other things of various violations of the GDPR and the Telecommunications Act. There is also no question of a legal act in which the Victims on the one hand and Oracle and/or Salesforce on the other hand are parties which could justify the enrichment. The Foundation explained above in chapter 4 that Oracle and Salesforce are wrongfully processing the personal data of the Victims.

5.8.6. Amount of the claim

786. Given the above, the Foundation (more in the alternative) takes the view that the compensation or the surrender of the wrongly enjoyed benefit can be based on a claim arising from unjustified enrichment.

787. The Foundation takes the view that the extent of the damage or the surrender of the wrongly enjoyed benefit has to be (abstractly) estimated (using extrapolation) at an amount of € 500 per person, as described above and in detail in chapter 5.

5.9 Joint and several liability

5.9.1 *Joint and several liability on the grounds of the GDPR*

788. Article 82 paragraph 4 GDPR states the following:

> *"Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. The party paying the total amount of the damage may recover (a part of) the amount paid from the other organisations involved."*

789. The foregoing shows that multiple parties are involved in the processing by Oracle and Salesforce. Primarily, the defendant Oracle and Salesforce entities are each the controller for their DMP processing and are jointly and severally liable for the entire damage suffered in

[542] *J. Spier, Commitments under the law and compensation,* (Study series Civil law part 5), Deventer: Kluwer 2015, page 380. E.F.D. Engelhard & G.E. van Maanen, Liability for damage contractual and non-contractual, Deventer: Kluwer, 2008, monographs Dutch Civil Code no. A15) p. 49.
[543] E.F.D. Engelhard & G.E. van Maanen, Liability for damage contractual and non-contractual, Deventer: Kluwer, 2008, monographs Dutch Civil Code no. A15) p. 49.

connection with their DMP service on the basis of Article 82 (4) GDPR. Insofar as there is joint responsibility with Publishers or Advertisers for part of the processing (margin number 284), it also applies that each of the parties involved is jointly and severally liable for the entire damage suffered in connection with those processing operations. In that case, for cookie syncing, Oracle and Salesforce are the controller together with the parties with whom they exchange data. Now that they also exchange data with each other in this context, Oracle and Salesforce and all other parties involved are each jointly and severally liable for all damage caused by cookie syncing (margin number 284).

5.9.2 Joint and several liability based on the Dutch Civil Code

5.9.2.1 Introduction

790. Insofar as Oracle and Salesforce argue that they do not bear full liability because other parties also contribute to the processing, Oracle and Saleforce moreover are each jointly and severally liable for the processing operations in connection with their DMP service pursuant to Article 6:166 of the Dutch Civil Code. Article 6: 166 of the Dutch Civil Code contains an (additional) rule on causal connection, concerning a wrongful act committed by one of the persons belonging to a group. [544] Primarily, the Foundation alleges that Oracle and Salesforce bear the primary responsibility. In the alternative, it can be stated that they each form such a group with the parties that use and/or contribute to their DMP processing.

791. For liability on the basis of Article 6: 166 of the Dutch Civil Code, four requirements must be met: (i) there must be action in a group context, (ii) participation of a group member in the conduct in a group context must result in a wrongful act. (iii) participation of a group member in the conduct in a group context must be attributable to him as a wrongful act and (iv) the act causing the damage must constitute a wrongful act towards the injured party.[545]

5.9.2.2 Group context

792. The Foundation is not required to put forward and, if necessary, to prove that there is a causal connection between the participation of Oracle and Salesforce in the group and the damage inflicted by one of the participants in the group. Oracle and/or Salesforce also cannot release themselves from liability by arguing and proving that there is no causal connection because the damage would have been caused even without their participation in the group. It is sufficient for assuming liability that one of the participants in the group has caused damage to the victims.[546]

793. To meet requirement (i), Oracle and Salesforce must have contributed to the conduct that created the risk of damage (the objective criterion). Oracle and Salesforce are not required to have actually cooperated in causing the damage. In addition, there must be a conscious joint action by the participants, whereby intent aimed at inflicting the damage is not required, but

[544] Asser/Hartkamp & Sieburgh 6-IV 2015/127.
[545] Asser/Hartkamp & Sieburgh 6-IV 2015/127.
[546] R.J.B. Bonnekamp, *Stelplicht & Bewijslast* (Obligation to furnish facts & burden of proof), Wrongful act in group context in connection with: Dutch Civil Code Book 6, Article 166.

the joint action increases the chance of damage and this chance is consciously accepted by the participants (the subjective criterion).[547]

794. Requirement (i) is met. Oracle and Salesforce act in a group context, now that they offer their DMP services to a large group of users and thereby engage in cookie syncing in a system (RTB) that is characterised by a high degree of interdependence.

795. As already explained in section 5.1, Oracle and Salesforce play an indispensable role in this data collection. As DMPs, they form the central data hubs in the advertising market. In that context, collaboration takes place between the various parties on the RTB market by means of cookie syncing, the phenomenon with which AdTech companies can easily exchange Cookie IDs (see section 3.2.6). This is one of the core activities of Oracle and Salesforce. Within this group, Oracle and Salesforce exchange Cookie Ids, other online identifiers and associated personal data on a large scale. On the basis of the identifiers, the parties involved can always easily communicate about the same user in order to obtain the most complete possible picture of that person. The participants in the group therefore consciously work together to collect as much personal data as possible for commercial purposes. There is thus a group that consciously acts jointly.

5.9.2.3 Wrongful act

796. The aforementioned actions of Oracle and Salesforce and their contributions to the RTB market also constitute a wrongful act. This also fulfils requirement (ii). Oracle and Salesforce should have anticipated that cookie syncing would increase the likelihood that Victims would lose control of their personal data and their privacy interests would be harmed. Even more so, they should have foreseen that this would actually cause the Victims to lose control over their personal data because they are unlawfully processing personal data. This should have made Oracle and Salesforce refrain from their actions.[548] Oracle and Salesforce have knowingly accepted the increase in the risk of damage to the Victims.

5.9.2.4 Attributability

797. The acts of Oracle and Salesforce in group context can also be attributed to them (requirement iii). As a matter of fact, each of the participants in this group, and certainly Oracle and Salesforce, can decide to discontinue these activities. By not doing that, but instead remaining commercially active in this group, the wrongful action can be attributed to each of them.

5.9.2.5 Wrongful act against the Victims

798. Finally, the actions of the group that caused the damage constitute a wrongful act against the Victims (requirement iv) (see section 8.1). Oracle and Salesforce, as participants in the group, are responsible for large-scale processing of personal data of internet users on the RTB market in violation of the GDPR and the Tw.

799. The Foundation is therefore of the opinion that Oracle and Salesforce are jointly and severally liable on the basis of Article 6: 166 of the Dutch Civil Code.

[547] Asser/Hartkamp & Sieburgh 6-IV 2015/127.
[548] Asser/Hartkamp & Sieburgh 6-IV 2015/127.

6. EXPLANATIONS OF THE RELIEF SOUGHT

6.1 Settlement of Damages Claims in Collective Proceedings Act (WAMCA)

800. The events to which the claims brought by the Foundation relate are encompassed in the new Settlement of Damages Claims in Collective Proceedings Act (*Wet afwikkeling massaschade in collectieve actie* : WAMCA)[549] It follows from Article 119a paragraph 1 of the New Civil Code Transition Act that the new law applies to collective proceedings which were instituted on or after 1 January 2020 for events which took place on or after 15 November 2016.

801. The General Data Protection Regulation (GDPR) (known in the Netherlands as the 'AVG') has applied throughout the whole of the European Union since 25 May 2018. Right from the start, Oracle and Salesforce have infringed the GDPR. Therefore, this involves events which took place after 15 November 2016, meaning that the new law applies.

802. The case in question only relates to acts after the GDPR became applicable, i.e. also after 15 November 2016.

6.2 Description of the groups of Victims

803. Pursuant to Article 3 paragraph 1 of its Articles of association (**Exhibit 2**), the Foundation represents the interests of:

> *"(...) natural persons who use the internet by surfing the internet and/or by using products and/or services which may store, transfer or process personal data in a digital form, leading at any time in respect of those internet users a violation of their right to protection of their privacy or their right to protection of their personal data takes place or did take place, all this within the broadest meaning."*

804. The outcome of these proceeding binds all of these persons, unless they choose to opt out (under Article 1018f of the Code of Civil Procedure). The majority of the Victims have their habitual residence in the Netherlands.

805. The group of persons represented by the Foundation falls into two categories (as far as this dispute is concerned), namely the group disadvantaged by Oracle and the group disadvantaged by Salesforce. Together they form a "Narrowly Defined Group" as meant in the WAMCA ("**Narrowly Defined Group**"). These two groups can be defined as follows:

a. The group disadvantaged by Oracle (further herein the '**Oracle Group**') which relates to:

   i. all natural persons

   ii. who have or have had the use of one or more computer(s) with internet access or other peripheral equipment within the sense of the Tw, and

[549] Dutch Act dated 20 March 2019 to amend the Dutch Civil Code and the Dutch Code of Civil Procedure in order to make possible the settlement of large-scale damage in a class action (WAMCA Act) (Dutch Bulletin of Acts and Decrees 2019/130). The WAMCA Act came into force on 1 January 2020 by Dutch Royal Decree dated 20 November 2019.

iii. on which a cookie called '**bku**' is or was placed,

iv. at a moment or during a period that they lived or resided in the Netherlands after the GDPR became applicable.

b. The group disadvantaged by Salesforce (further herein the '**Salesforce Group**') which relates to:

i. all natural persons

ii. who have or have had the use of one or more computer(s) with internet access or other peripheral equipment within the sense of the Tw, and

iii. on which a cookie called '**bku**' is or was placed,

iv. at a moment or during a period that they lived or resided in the Netherlands after the GDPR became applicable.

806. The Foundation will request the District Court to determine that:

a) each member of the Narrowly Defined Group living in the Netherlands or who has lived there for a period of three months after the announcement, within the meaning of Article 1018f paragraph 3 of the Code of Civil Procedure, to appoint the exclusive representative, will have the possibility to inform the registry of the District Court in writing to withdraw from the representation of their interests in these collective proceedings (opt-out);

b) each member of the Narrowly Defined Group who resides outside (or has a permanent address outside) the Netherlands will have the option - during a period of six months following the announcement within the meaning of Article 1018 paragraph 3 Rv of the ruling to appoint the exclusive representative – of letting it be known by means of a written message to the court registry whether he or she consents to his/her interests being represented in this collective claim (opt in).

6.3 Exclusive representative

807. In Chapter 8 'Admissibility of the Foundation' the Foundation will explain that it meets the admissibility requirements. This results in the Foundation bringing class actions purporting to appoint the Foundation as the exclusive representative within the sense of Article 1018e of the Dutch Code of Civil Procedure ('Rv').

6.4 Explanation of the claims

808. The Foundation will bring various claims in this action.

a. Claim I relates to the appointment of the Foundation as the exclusive representative.

b. Claim II relates to the determination of the Closely Defined Group to which this case relates. All this has been explained in the body of this Writ and in particular in section 6.2 above.

c. Claim III relates to the provision by the court that persons who do not wish to join this collective action, should make this known in good time in a way to be prescribed by the court (opt out) and the way in which foreign Victims can make it known that they do want to join (opt in).

d. Claim IV relates to the establishment of the joint and several liability of Oracle and Salesforce to each member of the Oracle Group and the Salesforce Group, pursuant to violation of the GDPR and the TW as comprehensively described in the body of this Writ.

e. Claim V concerns the order for compensation of damage, resulting from the violation of the GDPR and the Tw - as described in detail in the body of this Writ - , payable to the Oracle Group based on 10 million members as a lump sum (10 million times €500 = €5 billion) at any rate €500 per person, or at least the damage to be determined in the follow-up proceedings for assessment of the damage and payable to the Salesforce Group, assuming 10 million members as a lump sum (10 million times €500 = €5 billion) or at least €500 per person, at any rate the damage to be determined in the follow-up proceedings for assessment of the damage. Damages are claimed jointly and severally from both for the Oracle Group and the Salesforce Group, at any rate from each of them, with regard to the Oracle Group and the Salesforce Group respectively. The damages are based on Article 82 GDPR (directly, see paragraph 5.5 above) as well as Article 6:162 of the Dutch Civil Code (*Burgerlijk Wetboek:* 'BW') (wrongful act, section 5.7.1) and Article 6:212 of the Dutch Civil Code (unjustified enrichment, section 5.8). The body of this Writ has already described in detail that i) Oracle and Salesforce collect and process data from almost every Dutch internet user and ii) in 2019 approximately 13.25 million inhabitants of 12 years of age or older use the internet almost daily. It is therefore likely that the Oracle Group and the Salesforce group will consist of at least 10 million members). The amount of the damages claimed amounts to €500 for each member of the Oracle Group and €500 for each member of the Salesforce Group (section 5.5.4.2) , and this represents immaterial and/or material damage (section 5.5.3 and 5.5.5), estimated on a fixed (section 5.5.4.2) or abstract basis (section 5.7.6.2), or on the basis of handing over profit (section 5.7.6.1) and unjustified enrichment (section 5.8). The nature of the claim pursuant to Section 3:305a of the BW involves the possibility to pay the total amount to the Foundation, and then to order the Foundation to divide it.

f. Claim VI concerns the order for payment of compensation in respect of the data breach at Oracle, to the members of the Oracle Group and or Salesforce Group whose data was (possibly) accessible during the security breach reported in June 2020 (section 5.8.4). The damage thus caused is estimated at a fixed rate of EUR 100 per member of the Oracle Group and/or Salesforce Group, or at any rate the damage to be determined in follow-up proceedings for assessment of the damage. That there is damage has been alleged and is sufficiently clear. The nature of a claim on the basis of Article 3: 305a of the Dutch Civil Code means that it is possible to pay the total amount to the Foundation, and subsequently to charge the Foundation with the distribution thereof.

g. Claim VII and claim VIII relate to the claim to provide information by Oracle and Salesforce. They have insight into the way in which and with regard to whom they violated the GDPR and it is for the Foundation and the Dutch internet users many times more burdensome to map this at individual level. It is not unusual in collective actions that the burden of identifying the injured parties is placed on the defendant (ordered to pay) (see section 7.4). It is relevant for identification of the persons against whom violation of personal data protection took place, that insight is required into whose PC had a cookie placed in it and with regard to whom data was collected in other ways. This is sometimes demonstrable from the peripheral equipment of the respective Dutch internet user, but this will not always be the case. In view of this and the division of the funds, the Foundation claims that Oracle and Salesforce is to disclose information available at them about whose personal data they process (Claim VII). The same applies to the data about the (category of) persons who were disadvantaged by the security breach at Oracle, the nature, cause, extent and duration of the breach as well as the compromised data (Claim VIII). With a view to these information obligations the Foundation claims a penalty (Claim IX), as an incentive for performance, amounting to €1,000 per day for each failure.

h. Claim X relates to the claim for reimbursement of the costs of the action and for awarding other reimbursements. Pursuant to Section 1018l of the Code of Civil Procedure the court may deviate from the ordinary cost awarding rules in the event of the plaintiff's claim being awarded (in whole or in part) (Section 1018i Rv), in other words: award more, such as the actual costs. Please refer to section 6.7.2. The Foundation is willing to substantiate the costs it incurred by submission of all the required documents, all this at a later stage of the proceedings. In this connection the Foundation also claims reimbursement of the fee stipulated by the Funder (please refer to section 6.6).

i. Claim XI relates to the Foundation's proposal with regard to the way in which to settle the damage. The Foundation assumes here that both the Oracle Group as well as the salesforce Group consist of at least 10 million persons. It may be the case that not everybody will claim within due time the compensation they are entitled to. The Foundation proposes that in line with its corporate objective it will hand over any surplus to a non-profit organisation which is active in the area of privacy protection, and it would therefore not revert to Oracle and Salesforce. This is different with regard to the amount claimed by the Foundation that Oracle and Salesforce must pay to the Foundation in order to provide for the costs of settling the payment of the compensation to the Oracle Group and the Salesforce Group, by engaging a professional claim settler (see section 6.5 below): any surplus from this should indeed revert to Oracle and Salesforce.

6.5 Possible constructions for payment of damages and/or reaching a settlement

809. The aim of the Foundation is to generate compensation for its supporters. It has to incur considerable costs to this end. However, those costs are insignificant when compared with the total compensation which is claimed from Oracle and Salesforce: assuming that 10 million

Victims are eligible for compensation (at least once) of €500 per person, the damages amount to at least €5 billion for each defendant.

810. Compensation of such large amounts for so many people requires customised work. Experience has been gained under the WCAM with regard to settlements declared generally binding, such as in the Dexia case or AEGEAS.[550]

811. As far as the Foundation is concerned it is preferable if the parties reach a suitable solution in consultation with Your Court. In the alternative scenario that Your Court decides unilaterally on the way in which the compensation is to take place, the practical problems and big expenses associated with the settlement of such a collective action might not be sufficiently taken into account.

812. The Foundation imagines that, if its claims are awarded, Oracle and Salesforce transfer the total amount of the compensation to the Foundation, which will subsequently divide it. To this end the Foundation will engage a professional third party, such as for instance Computershare.[551] Such parties have a very significant track record with the settlement of collective actions, particularly in the United States but also in the meantime in the Netherlands. The role of the claim settler is in particular the identification of the parties who are entitled to compensation, and the payment of compensation. In this case it involves millions of people, which means that possibly millions of people have to be identified and might have to submit further documentation to demonstrate that they are a member of the Closely Defined Group and are eligible for compensation. This requires a considerable effort with regard to information technology as well as human work. Experience has shown that the costs of such an operation can easily cost €10 million or more and take a lot of time.

813. The Foundation imagines that, if its claims are awarded, Oracle and Salesforce will pay the Foundation (i) the various cost awards, the reimbursement of the Funder's fee and an advance for the costs of the claim settler of for instance €15 million and (ii) the compensation. The amounts under (i) will be paid/passed on or retained by the Foundation itself and the amounts under (ii) will be administered by the claim settler, on the instructions of the Foundation.

814. It may be possible that a dispute arises between the Foundation and/or the claim settler on the one hand, and a person who demands payment on the other hand. The Foundation imagines that Your Court will determine that anyone who wants payment, would submit to dispute settlement on the basis of a binding third party ruling and that the parties would express their opinion on this further in a court document.

6.6 Funder's fee

815. The Foundation did not ask a fee from the Victims but financed its costs by using an external Funder. The Funder bears the full litigation risk and the risk that the costs incurred cannot be earned back. In exchange the Funder asks a result-dependent fee (a commission) ranging

[550] Appeal Court of Amsterdam, 25 January 2007, *NJ* 2007, 427; Appeal Court of Amsterdam, 13 July 2018, ECLI:NL:GHAMS:2018:2422.
[551] https://www.computershare.com.

between25%, 15% or 10% of the compensation to be received by the Foundation for the Closely Defined Group.

816. It follows from the legal history that the Foundation can be reimbursed for the Funder's costs pursuant to Section 6:96 of the BW and pursuant to Section 1018l subsection 2 Rv: [552]

> *(...) if an external Funder is involved, he will pay in general also the costs of the exclusive representative. Section 6:96 of the Civil Code and Section 1018l of the proposal can then be used to have the Funder's costs reimbursed.* (...)".

817. Oracle and Salesforce should also be charged the fee which the Funder stipulates for his willingness to finance the costs of the proceedings and to run the litigation risk.[553] Therefore the Foundation claims that the Funder's costs as well as the fee the Funder stipulated will be at the expense of Oracle and Salesforce pursuant to Section 1018l subsection 2 Rv or Section 6:96 BW. In the relief sought this fee is claimed pursuant to Section 6:96 BW as well as pursuant to Section 1018 subsection 2 Rv, but no double counting is intended.

818. The fee stipulated by the Funder is reasonable in view of the actual activities carried out and the litigation risk it runs. The Funder has made substantial investments and expenses by financing all the costs of the Foundation, that is to say, the costs with regard to the investigation of the facts, legal research, remuneration for the Board and Supervisory Board, the costs of setting up and maintaining websites and data bases, costs of other advisors such as the civil-law notary, the tax consultant, accountant and also the costs of the advocate. In addition, it is common practice that a Funder charges a fee. Collective actions can be very expensive. However, it is of social importance that collective actions can be brought so that usually funding has to be found for it. The Funder usually asks a result-dependent fee in exchange for the costs incurred and the litigation risk it runs, as is the case here. On the other hand the Foundation does not ask a financial contribution from the Victims. The Victims can join the Foundation free of charge and may profit from its activities.

819. In addition, the Foundation also complies with the Claim Code. After all, the Claim Code allows the Foundation to raise external financing and the Foundation to agree a fee with the external Funder based on a percentage of a collective compensation/fee to be awarded in or outside court:[554]

> *"(...) If the external Funder is entitled to a fee based on a percentage of a collective compensation/fee, the representative organisation shall also state the respective percentage."*

820. It follows from the foregoing that the interests of the Victims are thus represented with due care and the fee which the Funder stipulated would have to be at the expense of Oracle and Salesforce.

---

[552] See also Parliamentary Documents (*Kamerstukken*) II 2017/18, 34608, no. 9. 5; Parliamentary Documents II 2017/18, 34,608, no. 9, p. 14.
[553] See also M.W. Schonewille, ''About litigation funding: relevant practical and legal aspects' *TOP* 2019/325, number 6. October 2019.
[554] Claim Code Principal III, elaboration 7.

6.7 Order to pay the costs of the proceedings

6.7.1 Specification of the costs of the proceedings

821. The Foundation wants to receive reimbursement for its costs of the proceedings. These costs include the costs of the bailiff, the fixed court fee, costs of the advocate and the costs of and the fee to the Funder.

822. The Foundation reserves the right to add to the specification of the costs of the proceedings an overview of the costs incurred/still to be expected after this Writ has been issued.

823. The Foundation will explain below that it can claim reimbursement of the costs of the proceedings pursuant to Section 1018 subsection 2 Rv and/or Section 237 Rv.

6.7.2 Article 1018l subsection 2 Rv

824. Section 1018l subsection 2 Rv provides for the costs of the proceedings in actual fact incurred, including, but not limited to the costs of the advocate which derogates from Section 237 Rv. With the words "a judgement pursuant to Section 1018i" the derogating arrangement to pay the costs of the proceedings only applies in the event that the court passes a judgement in which it establishes a collective claim settlement. Thus the legislator created explicit scope for the court to reimburse the costs incurred by the Foundation and to shift them to the defendant [555]. Also the fee payable by the Foundation to the Funder can be charged to the defendant in this way, as explained above[556]. Therefore the Foundation claims pursuant to Section 1018l subsection 2 Rv that Oracle and Salesforce be ordered jointly and severally to pay the reasonable and proportionate court costs and other costs which the Foundation has incurred.

6.7.3 Section 237 Rv

In the event that the collective claim settlement is rejected and only the declaratory judgements are awarded, the Foundation claims primarily that Oracle and Salesforce be ordered jointly and severally to pay the costs of the proceedings actually incurred pursuant to Section 1019h Rv and in the alternative a joint and several order to reimbursement of the costs of the proceedings incurred pursuant to Section 237 Rv.[557]

6.8 Order to pay extra-judicial costs

825. The Foundation also claims reimbursement of the full (extrajudicial) costs incurred pursuant to Section 6:96 BW, including the costs of the Funder[558], insofar as they had not already been taken fully into account on the basis of Section 1018l lid 2 Rv.

---

[555] Parliamentary Documents II, 2016/17, 34 608, no. 3, p. 54.
[556] Parliamentary Documents II, 2017/18, 34 608, no. 9, p. 14.
[557] See also on joint and several order to pay the costs of the proceedings under Article 237 of the RV: Text & Comment on Civil Procedure, Costs Decision, in general with regard to: Code of Civil Procedure. Article 237; See also the confirmation of this in: Asser Procedural Law / Van Schaick2 2016/136.
[558] *Parliamentary Documents II*, 2017/18, 34 608, no. 9, p. 14, where it is explicitly considered that these costs are also eligible for reimbursement pursuant to Section 6: 96 BW.

826. These costs consist of the costs incurred and still to be incurred by the experts and the costs of legal advice incurred and still to be incurred. These costs also consist of the costs to obtain reparation out of court pursuant to Section 6:96 subsection 2 c BW.

827. In total the extrajudicial costs consist of the amount of €10 million, excluding the fee which the Foundation will owe to the Funder. Considering the circumstances of this case the activities performed were reasonably necessary and the costs in terms of the amount are reasonable.[559] The Foundation acts for the benefit of 10 million people who jointly have a claim which is many times greater than the costs incurred by the Foundation. The individual members of the Closely Defined Group are unable to obtain redress in a comparable efficient way, given the compensation being relatively low - in comparison with the costs of investigation and legal costs to be incurred by them.

7 EVIDENCE

7.1 Introduction

828. The claims of the Foundation are based in particular on the following facts and allegations:

a) Oracle and Salesforce are processing without any basis the data of Dutch internet users in connection with their DMP service and collecting and processing data in other ways by placing cookies without sufficient consent (see section 4.6.1);

b) Oracle and Salesforce do not provide adequate information with regard to the use of cookies, cookie syncing and further processing in connection with providing the DMP service (see section 4.6.3 “Processing not transparent”);

c) Oracle and Salesforce collect, combine and share limitlessly and excessively any personal data (see section 4.6.4 “Processing contrary to data minimisation”);

d) Oracle and Salesforce pass on personal data to the United States, where no suitable level of protection can be offered (see section 4.6.5 "Prohibited transfer to the United States");

e) Oracle has not taken any adequate technical or organisational measures to adequately protect personal data. This is evident from Oracle's data breach in 2020 causing millions of personal data which it collected to be exposed (see section 4.7 “Oracle protects personal data inadequately, according to a data breach in 2020”); and

f) The Victims are suffering (any form of) damage by the infringing actions of Oracle and Salesforce.

829. The Foundation is of the opinion that it has put forward more than enough in this Writ with regard to each of these facts and allegations. At the same time it is a fact that a large part of the factual course of events has escaped the observation of the Foundation (and the internet users) and that this cannot be traced even by the external specialists engaged by the Foundation, without the cooperation of Oracle and Salesforce itself. After all, the processing operations in

[559] See also the Memorandum of Reply II, Parl. History 6, p.337.

connection with the DMPs largely take place "behind the scenes" on the servers and in the systems of Oracle and Salesforce in particular, to which the Foundation has no access. However, the Foundation does not have to put forward exactly and prove exactly how the DMP activities work and which role each of the participants performs in this connection. This does not constitute support for the claims brought by the Foundation and the obligation to furnish facts/the burden of proof does not rest on the Foundation.

7.2 Starting points under the law of evidence

830. Neither does the Foundation have to prove that Oracle and Salesforce violated the principles of the GDPR. The Foundation explained above that in the present case the following starting points under the law of evidence should apply (see among other things section 4.3.2.2, 5.2.1, 5.2.2 and 5.2.3 and margin numbers 401, 412 and 624):

- Oracle and Salesforce are presumed to process personal data under the Tw;
- Oracle and Salesforce are a controller within the sense of the GDPR. If Oracle and Salesforce are of the opinion that they are not a controller, they have to demonstrate this;
- The burden of proof with regard to the compliance with the GDPR rests on Oracle and Salesforce;
- Oracle and Salesforce must (on the basis of the transparency obligation) provide clarity about who is the controller and who is otherwise (as source or recipient) involved in the processing of the personal data*;*
- Even if Oracle and Salesforce were only the processor under the GDPR and even if there would be no processing of personal data, they have the burden of proof under Article 11.7a Tw to demonstrate that consent has been obtained and information was obtained and that that consent and information comply with the GDPR, because they placed the cookies; and
- The causal connection (CSQN connection) is already presumed due to the violation of the GDPR by Oracle and Salesforce.

831. In this case Oracle takes the position that it should only be considered as the processor for its DMP service (see below in chapter 10 ‘Known defences and refutation’). In this Writ, the Foundation has already explained with reasons that this allegation is incorrect. As stated above, the basic principle is that Oracle must demonstrate that it is not a controller.

832. In addition, Oracle's defence that it is only a (partial) processor qualifies as an "independent" or "discharging" defence. This means that Oracle bears the burden of proof of the facts and circumstances underlying its defence. Also with regard to Salesforce, if Salesforce takes the position that it should only be regarded as a processor, Salesforce will bear the burden of proof of the underlying facts and circumstances.

7.3 In the alternative: request to furnish proof by an expert report to be ordered pursuant to Article 194 Rv

833. In the unlikely event that the Court holds that any burden of proof falls on the Foundation, the Foundation requests the Court to be allowed to provide evidence by means of expert advice. The Court has a discretion as to whether or not to order an expert report.

834. In this connection, the Foundation notes that it must be taken into account that the Victims suffered damage as a result of the infringing acts of Oracle and Salesforce and that this damage must be compensated. However, much of the infringing activity takes place behind the scenes at Oracle and Salesforce. By analysing all kinds of information, the Foundation has been able to paint a picture of what Oracle and Salesforce do behind the scenes. However, the Foundation does not have all the relevant information and data in this case. The only way to obtain all the data, if necessary, is through the infringing parties themselves, namely Oracle and Salesforce.

835. The Foundation therefore requests Your Court to engage an expert if necessary pursuant to Article 194 Rv. The expert can (among other things) conduct research into:

- The role of Oracle and Salesforce in the RTB system;
- How exactly the DMP activities work, and exactly what role each of the participants play in this;
- Which DMP activities Oracle and Salesforce perform;
- How exactly Oracle and Salesforce process the personal data of the Victims;
- Which personal data exactly Oracle and Salesforce process;
- How long Oracle and Salesforce retain personal data;
- The way in which Oracle secures the personal data;
- The value of the personal data wrongfully processed by Oracle and Salesforce.

7.4 In the alternative: other possibilities of obtaining necessary information in the present case

836. If and insofar it would be established that the burden of proof rests on the Foundation and it has not (yet) been successful in furnishing evidence, the Foundation sees reasons that it should be accommodated in the area of law of evidence in these proceedings for the benefit of the Victims. Section 150 Rv and the rules of written and common law make this possible. The seriousness of the acts of Oracle and Salesforce, as comprehensively discussed in this Writ and the nature of the claims of the Victims and the circumstances of the case give rise to that. It also applies that the interests of the Victims to obtain more clarity and information significantly outweigh the interests of Oracle and Salesforce to keep their (infringing) actions secret.

837. The facts largely take place behind the scenes at Oracle and Salesforce. It is thus necessary that they disclose the relevant information and data. There are other ways for the Court to give shape to this in the event that Oracle and Salesforce do not disclose the necessary information. They will be explained one by one below.

a. Based on general rules of experience a factual presumption can be assumed to the disadvantage of Oracle and Salesforce;[560]

i For instance, considering (the nature of) the actions, the motives and the infringement of Oracle and Salesforce, it can already be assumed on the basis of a presumption that the Victims have suffered damage as a result.

b. The burden of proof can be divided or reversed in accordance with reasonability and fairness;[561]

i. The Court may reverse the burden of proof onto Oracle and Salesforce in connection with the allegations of the Foundation with regard to the infringement, the wrongful act of Oracle and Salesforce, and the extent of the damage this inflicted on the Victims.

c. Oracle and Salesforce could be burdened with an increased obligation to furnish facts or duty of justification in order to relieve the lack of evidence of the Foundation;[562] and

i. The Foundation establishes that in this case Oracle and Salesforce - unlike the Victims and the Foundation - have the relevant information and data at their disposal, at any rate more information than the Victims and the Foundation have. A large part of the factual course of events has escaped the observation of the Foundation and the internet users. Oracle and Salesforce have the information on how they participate in the RTB system, which DMP activities they carry out and in exactly what way they process the personal data of the Victims and violate their privacy. Therefore the Foundation takes the position that (in any case) an increased obligation to furnish facts (duty of justification of the defence) ought to rest on Oracle and Salesforce.

d. The Court may also make use of the reversal rule with regard to the causal connection in relation to the wrongful act; [563]

i. The Foundation primarily takes the position that the existence of a causal connection (in the sense of the CSQN connection) between the wrongful act of Oracle and Salesforce and the damage is assumed since Article 6: 162 BW (and Article 6:98 BW) should be interpreted in compliance with the GDPR (section 5.7.5).

ii. In the alternative, the Foundation takes the position that if the GDPR-compliant interpretation is not followed, the existence of the CSQN connection between the

[560] Asser Procesrecht (Procedural law) 3 Bewijs (Evidence) 2017/304; Asser/Vonken 10-I 2018/193.
[561] Asser Procesrecht (Procedural law) 3 2017/291.
[562] Asser Procesrecht (Procedural law) 3 Evidence 2017/306 and 307.
[563] Asser Procesrecht 3 2017/302.

wrongful act of Oracle and Salesforce and the damage must also be assumed in that case, now that there is a violation of a standard that aims to prevent a specific risk and that this specific risk has materialised (section 5.7.5).

7.5 Duty to state the truth (Article 21 Rv)

838. Moreover, arriving at the truth is a fundamental principle of procedural law (Article 21 Rv). This can only be interpreted in a meaningful way in court with an as much as possible complete and correct establishment of the facts. Therefore the parties have a duty to state the truth and be complete. The court has the duty to pronounce judgement on the basis of the reality (arriving at the truth). This can be translated as the litigation parties having with regard to each other also rights to obtain and provide information.[564] They can claim that information which is relevant for them and which is only at the disposal of the counterparty, should not be withheld from them.[565] They put forward what is important for the dispute. Parties have no right to silence and can be obliged to produce evidence against themselves in a legal action or to testify against themselves.[566]

839. With much of the present Oracle and Salesforce actions taking place behind the scenes, it stands to reason that Oracle and Salesforce will in this connection be obliged to provide the information that they have at their disposal, including detailed information about how they have set up their servers and systems. This also ties in well with the principles of transparency and accountability discussed above.

7.6 Acts of evidence pursuant to Article 22 Rv

840. It is against this background that the legislator gives the court itself the power to take, officially, the initiative in obtaining evidence (Section 22 Rv). The court can ask the parties questions, order them to produce documents, appoint an expert to inform the Court, view situations onsite and examine witnesses. This means that the court is not completely dependent on what the parties submit in terms of evidence and supporting information. In this way the court can also encourage the arriving at truth of good quality and thereby the quality of the process as well as the judgement.[567]

841. In this way weaker parties such as the Victims, could be helped to obtain justice against a stronger counterparty (such as Oracle and Salesforce). For that matter by the indication of "weaker parties" the Foundation does not only mean the position of a single person, after all it could be put forward on the part of Oracle and Salesforce that the Foundation is not as weak as an individual internet user. It is about the position of the party who has been disadvantaged because it does not have the information and documents at its disposal which may be determinant for the grounds of the claim, whereas the counterparty does have this information at its disposal. It is a question of information asymmetry which might lead to lack of evidence on the part of the individual internet users and the Foundation. That knowledge is within the sphere of Oracle and Salesforce and it is up to them to further substantiate any challenge. The

[564] Asser Procesrecht (Procedural law) 3 2017/41, Supreme Court 25 March 2011, ECLI:NL:HR:2011:BO9675, *NJ* 2012/627 (*Duty to state the truth*).
[565] Asser Procesrecht (Procedural law) 3 2017/29.
[566] Asser Procesrecht (Procedural law) 3 2017/40.
[567] Asser *Procesrecht* 3 2017/76.

Foundation may also for instance be unable to (completely) check the allegations of Oracle and Salesforce, as set out in the demand letter, due to the lack of information.

842. Particularly in the event that a plaintiff suffers from a structural lack of information (with regard to the duty to furnish facts), in particular in connection with proving the causal link and the damage because all the necessary information is situated in the sphere of the counterparty who challenges the claims and their grounds, it is necessary that the counterparty provides disclosure. If a defendant does not do this, the principles of fair play and equality of arms, as arises from Article 6 ECHR will be compromised.

7.7 Claim to provide information by Oracle and Salesforce

843. The Foundation has already explained on various occasions that there is an information asymmetry because a large part of the information is situated in the sphere of Oracle and Salesforce. Oracle and Salesforce know exactly the way in which they participate in the RTB system, which DMP activities they carry out and in what way they process the personal data of the Victims and violate their privacy. The Victims often don't even know that their personal data are being processed, let alone in what way. Oracle and Salesforce should be prevented from continuing with this unchallenged.

844. In their letters dated 18 June and 17 June and the conversations conducted on 7 July and 3 July Oracle and Salesforce dispute a part of the claims and the facts on which the Foundation based its claims. Particularly in that case and in view of the specific circumstances of this case, it is necessary that Oracle and Salesforce provide disclosure.

845. Therefore the Foundation claims that the information which is relevant to the claims being brought and which only Oracle and Salesforce have at their disposal, is not withheld from it.[568]

846. More specifically the Foundation brings a claim serving to obtain insight into the way in which and with regard to whom Oracle and Salesforce violated the GDPR and the Tw in connection with their DMP activities (which should also include the service which Oracle indicates as ADM). It is not unusual in collective actions that the burden of identifying the injured parties is placed on the defendant (ordered to pay) (see for instance 7.4). Insight into the persons who received a cookie for identification of the persons with regard to whom the GDPR has been violated, is relevant. This is sometimes demonstrable from the peripheral equipment of the respective Dutch internet user, but given the limited life of cookies this will not always be the case. In that case it may be relevant which websites were visited and when, because it can be deduced from this whether they would have received a cookie. In view of this and the division of the funds, the Foundation claims that Oracle and Salesforce is to provide this information. The same applies to the data of the persons who have been disadvantaged by the data leak at Oracle.

847. Apart from this the Foundation reserves the right to bring additional claims to obtain information about subjects mentioned in this Writ and other subjects.

848. That Oracle and Salesforce have to provide disclosure is also emphasised by the GDPR. If Oracle and Salesforce would not be ordered to provide this information, the protection which

[568] Asser Procesrecht (Procedural law) 3 2017/29.

can be derived from the GDPR will be in actual fact meaningless. One of the objectives of the GDPR is to guarantee the protection of natural persons with regard to the processing of their data. The GDPR also explicitly states that the data controllers, in this case Oracle and Salesforce, must demonstrate that they comply with the obligations that apply to them under the GDPR. Oracle and Salesforce must provide disclosure and give the required information and not evade (partial) liability by keeping that information to themselves.

849. In addition, the Foundation points out - needless to say - that in estimating the damage the court is not bound by the rules of the obligation to furnish facts and the burden of proof. If it can be deduced that the damage has been suffered, the court cannot reject out of hand the compensation for it due to a lack of substantiation of the amount of it.[569]

850. If the victim puts forward facts from which it can in general be deduced that damage has been suffered, the court will be free to consider it plausible without any further evidence - partly taking into account the nature of the damage - that damage has been suffered and to estimate the amount of it.

851. The Foundation takes the position that it has put forward sufficient facts in this Writ from which it can be inferred that the Victims have suffered damage. Oracle and Salesforce have collected and processed on a large scale and for commercial purposes the personal data of the Victims. Therefore they violated in a structural way among others the GDPR, the Tw and the privacy rights of the Dutch internet users. This means that the Victims lost control of their personal data. It can be deduced from these facts and circumstances that the Victims suffered damage. Considering its nature (loss of control of personal data) this damage should be eligible for compensation.

852. The Foundation substantiated in section 5.5.4-5.5.5 the amount of the damage. With a view to the foregoing the Foundation takes the position that in the event that the substantiation would be insufficient, the claims for compensation should also not be rejected.

853. In that connection the Foundation also points out that in estimating the damage Section 6:97 BW should be interpreted in compliance with the GDPR. This means that estimating the damage should do justice to the objectives of the GDPR. The starting point of the GDPR (recital 146) is that the damage must be interpreted broadly in view of the case law of the ECJ EU in a way that fully justifies the objectives of this Regulation. The data subjects should receive full and actual compensation for the damage they suffered. This starting point will also have to be followed in estimating the damage which the Victims suffered.

854. With regard to the Foundation's claim for damages which is based on handing over profit, the Foundation points out that it is extremely difficult to furnish facts and evidence of what amounts are involved. This information is not in the public domain. However, since estimating damages based on handing over profit is a discretionary power of the court, any specific disadvantage does not have to be demonstrated by the Foundation. It is sufficient that the presence of any (form of) damage is plausible. It is up to Oracle and Salesforce to make it

[569] Supreme Court 28 April 2000, ECLI:NL:PHR:2000:AA5651 (*Gemeente Dordrecht/Stokvast*).

plausible that no damage could have been caused as a result of the behaviour for which they are held liable.[570]

855. As already set out in margin numbers 734 et seq. the Foundation has no information at its disposal with regard to the profitability of the DMP activities on the RTB market for Oracle and Salesforce. It is true that (annual) figures they published show billions of euros revenue but they give insufficient insight into the revenues generated specifically with cookie syncing on the Dutch (RTB) market. Therefore the Foundation requests Your Court to order Oracle and Salesforce to produce specific information which allow at least an estimate of the profit from the advantage they enjoyed during the period from the moment that the GDPR became applicable.[571]

856. Finally, the Foundation further reserves the right to substantiate further the damage of the Victims during the course of these proceedings.

7.8 The Foundation offers to furnish evidence

857. If and insofar as the evidence is not yet considered fully furnished in respect of all components, the Foundation offers to furnish evidence of all its allegations by all means that are at its disposal. This also includes examining witnesses, appointing experts and producing further documents. In offering this, the Foundation does not accept voluntarily any burden of proof which does not rest on it.

8. ADMISSIBILITY OF THE FOUNDATION

8.1 General: the recent revision of Section 3:305a BW and the framework of standards currently applicable

858. The Foundation has brought this action on the basis of Section 3:305a BW. Section 3:305a BW was amended upon the Dutch Collective Damages in Class Actions Act coming into force.[572] With the Dutch Collective Damages in Class Actions Act coming into force the requirements for admissibility of interest groups who want to bring a collective action for a group of Victims have been tightened.

859. The requirements are particularly tightened to prevent inappropriate use of the collective action procedure.[573] This perspective necessitates a cautious attitude for the court when assessing the structure of an interest group. That usually does not restrain the parties who are sued in a collective action procedure from putting forward inadmissibility defences. Those

[570] Supreme Court 18 June 2010, ECLI:NL:HR:2010:BL9662, with annotation by T. Hartlief (Setel/AVR); Supreme Court 18 June 2010, ECLI:NL:HR:2010:BM0893 (Stichting Ymere); G. van Dijck & R. Olde Wolbers, Winstafdracht en het schadevereiste, mede aan de hand van een vergelijking met Zwitsers recht (Handing over profit and the damage requirement, partly on the basis of a comparison with Swiss law), WPNR, 2015, p. 2.
[571] Supreme Court 18 June 2010, ECLI:NL:HR:2010:BL9662, with annotation by T. Hartlief (Setel/AVR); Supreme Court 18 June 2010, ECLI:NL:HR:2010:BM0893 (Stichting Ymere); Groene Serie Schadevergoeding (Green series Compensation), 3 Generated profits as a criterion in connection with: Dutch Civil Code Book 6, Section 104.
[572] The Act of 20 March 2019 to amend the Dutch Civil Code and the Dutch Code of Civil Procedure in order to enable the settlement of mass damage in a collective action (Dutch Collective Damages in Class Actions Act) (Bulletin of Acts, Orders and Decrees 2019/130. The Dutch Collective Damages in Class Actions Act has come into force on 1 January 2020 by a Royal Decree of 20 November 2019.
[573] *Kamerstukken II* 2017/18, 34 608, 9, p.1.

defences will then mainly be put forward to avoid the principal issue.[574] It is not allowed to use an inadmissibility defence for this purpose.

860. Section 3:305a subsection 1 BW provides (among other things) that the interest group (i) may bring a legal action serving to protect similar interests of other persons ('similarity requirement'), (ii) insofar as it represents those interest in its articles (of association) (the requirement of articles') and (iii) by commencing a legal action the interests of the persons for whom a claim is brought have been sufficiently safeguarded ('the safeguard requirement'). The safeguard requirement is further detailed in Section 3:305a subsection 2 BW.

861. Section 3:305a subsection 3 BW contains several additional admissibility requirements. Paragraph a provides that directors involved in the incorporation of an interest group and their successors, should not have any direct or indirect profit motive that is realised through the interest group. Paragraph b contains the requirement that the collective claim has a sufficiently close connection with the Dutch legal sphere. Paragraph c provides that an interest group must have tried sufficiently in the given circumstances to achieve the redress by conducting consultations with the defendants.

862. The Foundation will first examine below the similarity requirement. Then the Foundation will discuss the requirement of articles. Then details will be given of why the Foundation is sufficiently equipped to represent the interests of the Victims or in other words the interests are sufficiently safeguarded. It will also be explained that the Foundation as well as its directors have no profit motive and that the claims have a sufficiently close connection with the Dutch legal sphere. Finally, it will also be discussed how sufficient efforts were made to bring about an out of court solution with Oracle and Salesforce, but that this was unsuccessful.

8.2 Similarity requirement

863. The power of interest groups to instigate legal actions pursuant to Section 3:305a BW is limited to the protection of similar interests. It follows from standard case law of the Supreme Court that the requirement of similarity is fulfilled when the interests, for the protection of which the claim relates, lend themselves to bundling, so that efficient and effective legal protection for the benefit of the interested parties can be promoted. The claims lend themselves to being put together if a judgement on it can be rendered in one single legal action without taking any special circumstances of the individual interested party into account.[575]

864. In any case, the interests of the Victims are similar now that (i) their personal data are being processed, and (ii) their privacy rights have been infringed, causing them damage, and (ii) the damage is caused by Oracle and Salesforce. The interests to which the claims relate can be generalized sufficiently to be counted among the similar interests to which Section 3: 305a of the Dutch Civil Code pertains. All the members of the Closely Defined Group, have in common that they are affected by the (wrongful) processing of their personal data by Oracle and Salesforce for merely commercial purposes on a large scale and over an unlimited time,

[574] See also K. Rutten, '*Art. 3:305a lid 2 BW schiet zijn doel voorbij!*' (Section 3:305a subsection 2 BW misses its mark!), MvV 2015/11.5, p. 324 and C.M.D.S. Pavillon & D.G.J. Althoff, 'Wijze raad is halve daad of veel raad maar weinig baat? (Wise counsel is half deed or much counsel but little benefit?) The impact of the Recommendations of the Lawyers' group to the legislative proposal 'Settlement of mass damage in a collective action', MvV 2017, p. 106.
[575] Supreme Court 26 February 2010, ECLI:NL:HR:2010:BK5756 (*Stichting Baas in Eigen Huis/Plazacasa)*.

without there being any justified ground for this and while the GDPR and Tw are being violated with regard to all the other points referred to above. Therefore, the privacy rights of all the members of the Closely Defined Group have been violated.

865. The claims as represented in section 6.4 require an abstract assessment, without additional individual circumstances having to be assessed. In this case, all Dutch internet users are dealing with exactly the same circumstance, namely that Oracle and Salesforce are violating the obligations under the GDPR and Tw and are acting wrongfully towards Dutch internet users, through the large-scale and unlimited processing of their personal data, without any ground for justification, transparency etc. The privacy interests of the Dutch internet users who are disadvantaged by this thus correspond with each other and they can therefore be put together. Therefore the claims lend themselves for assessment in a collective action.

866. It follows from the foregoing that the similarity requirement has been met.

8.3 Requirement of articles

867. The requirement of articles means that the interest to be represented is formulated in the articles of the Foundation and activities in the respective area have been engaged in.

868. The representation of the Victim's interests in these proceedings is within the scope of the corporate objects set out in the articles of the Foundation. As indicated, Article 3 paragraph 1 of the Articles (**Exhibit 2** provides in this respect:

"The object of the Foundation is to represent the interests of natural persons who use the Internet to surf the Internet and/or through the use of products and/or services that can store, transfer or process personal data in digital form, whereby on the part of those Internet users there is (or has been), at any time, a violation of their right to protection of their privacy or their right to protection of their personal data, all this in the broadest sense of the word."

869. Article 3 paragraph 2 of the articles lists the activities of the Foundation:

> *The Foundation seeks to achieve this goal by investigating the liability of parties who violate these rights of the persons whose interests are represented by the Foundation, by conducting negotiations, by supporting and initiating one or more legal actions in the Netherlands or beyond, including, but not limited to, proceedings as referred to in Section 305a of Book 3 of the Dutch Civil Code and Section 240 of Book 6 of the Dutch Civil Code, and by initiating other legal proceedings, including a claim for a declaratory judgement, by taking measures to address wrongful acts and by demanding appropriate compensation and redress, by making amicable settlements, by entering into a collective settlement agreement to terminate disputes, and by calculating and determining damages or having damages calculated and determined and by (continuing to) pay damages and by performing everything related to the above in the broadest sense or which may be conducive to this.*

870. The requirement of actual representation of interests has been met. The Foundation has not been idle and takes its tasks more than seriously. It has undertaken among others the following activities to represent the interests of the Victims:

- The Foundation conducts (technical) research into the privacy aspects of the large-scale collection and processing of personal data of internet users and the role of Oracle and Salesforce in this.
- The Foundation is continuously campaigning to combat the wrongful use of personal data of internet users in the Netherlands and abroad. To this end it created an umbrella campaign website: https://theprivacycollective.eu/nl/ on which additional information can be found about its activities in the Netherlands. Various articles and studies have also been published on this campaign website about AdTech, RTB, cookies and other tracking technologies and how companies wrongfully collect and use personal data by networks of online platforms;
- The Foundation also has a website specifically designed for the collective action in the Netherlands *(https://theprivacycollective.nl/)*. On it the Victims can find comprehensive information about the Foundation, its working method and activities and the Foundation offers the opportunity to ask questions;
- The Foundation has raised support from important interest groups in the Netherlands which aim to preserve and promote the right to privacy, such as Bits of Freedom, Privacy First, Freedom Internet and Qiy Foundation.
- The Foundation held consultations with Oracle and Salesforce. It had a discussion with Oracle on 7 July 2020. It had a discussion with Salesforce on 3 July 2020. See below under 8.5.4.

8.4 Guarantee requirement

871. Article 3:305a(1) of the Dutch Civil Code stipulates that the interests of those that the interest group represents must be sufficiently safeguarded. In addition, the guiding principles may not be ignored. These interest groups have the freedom to set up their own organisation.[576] Neither may the right of access to the court be restricted lightly.[577]

872. Article 3:305a(2) of the Dutch Civil Code defines and reinforces these requirements in more detail. Article 3:305a(2) of the Dutch Civil Code stipulates that the interests are sufficiently safeguarded when (i) the interest group is sufficiently representative, in view of the support base and the scope of the claims and (ii) the interest group meets a number of requirements in Claim Code 2019, which are codified in this paragraph. The Foundation will discuss these requirements below and explain that it meets these requirements.

8.4.1 (i) The Foundation is representative of the group of Victims

873. This relates to the extent to which an interest group can be regarded as representative of the group of Victims. Representativeness is important in order to avoid an interest group from bringing judicial proceedings without the required support of a support base.

[576] Partly due to the provisions of Article 11 of the ECHR.
[577] Partly in relation to the provisions of Article 6 of the ECHR.

874. Whether an interest group is sufficiently representative, can be derived from different data. A clearly-defined interpretation of this concept is not given, because it would not do justice to other data that may also indicate that an interest group is representative.

875. For example, one could consider the extent to which the Victims themselves see the organisation as being representative, the expertise and experience of the organisation, other activities carried out by the organisation, the number of affiliated Victims, the extent of their claims in relation to the total number of Victims in a mass event, and the damages claimed by them.[578]

876. It should be clear in advance that, in quantitative terms, the interest group represents a sufficiently large portion of the group of affected Victims. What is enough differs on a case by case basis, and can only be determined in relation to the total number of Victims. For example, this can be verified by means of the number of Victims that have actively signed up for the claim.[579]

877. It is sufficient to define precisely which group of people the interest group represents.[580] Pursuant to Article 3(1) of its Articles of Association (**Exhibit 2**), the Foundation represents the interests of:

> *"(...) natural persons who use the Internet to surf the Internet and/or through the use of products and/or services that can store, transfer or process personal data in digital form, whereby on the part of those Internet users there is (or has been), at any time, a violation of their right to protection of their privacy or their right to protection of their personal data, all this in the broadest sense of the word."*

878. In these proceedings, the Foundation represents exclusively those Internet users in the Netherlands. The Foundation's support base is thus formed (in principle) of all natural persons in the Netherlands who use the Internet. It appears from the figures of Statistics Netherlands (CBS) that in 2019 in the Netherlands, approximately 87.6% of Dutch persons aged 12 years and above use the internet practically every day.[581] In 2019 the Netherlands had 15,121,956 inhabitants aged 12 years and older.[582] 87.6% of this number is 13,246,833 persons. So in 2019 the Netherlands had approx. **13.25 million** inhabitants of 12 years or older who use the internet particularly every day.

879. The Foundation also has the support of leading interest groups in the Netherlands, such as the foundation Bits of Freedom[583] the foundation Privacy First, [584] Freedom Internet B.V.[585] and Qiy Foundation.[586]. These interest groups defend the interests and rights of Internet users in the Netherlands.

---

[578] *Parliamentary Papers II,* 2003/404, 29414, 3, p. 15.
[579] *Parliamentary Papers II,* 2016/17, 34608, 3, p. 19.
[580] *Parliamentary Papers II,* 2016/17, 34608, 3, p. 19.
[581] https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?fromstatweb.
[582] https://opendata.cbs.nl/statline/?dl=1EFBB#/CBS/nl/dataset/7461bev/table.
[583] https://www.bitsoffreedom.nl.
[584] https://www.privacyfirst.nl.
[585] https://www.freedom.nl/.
[586] https://www.qiyfoundation.org/

880. For years, the Bits of Freedom foundation has been committed to the better protection of personal data of Internet users in the Netherlands. Bits of Freedom was, inter alia, actively involved in the creation of the GDPR.[587] On 29 May 2019, it filed an enforcement request with the Dutch Data Protection Authority in the context of a systematic violation of the GDPR and an infringement of the rights of Dutch people in the RTB market.

881. The Foundation Privacy First aims to preserve and promote the right to privacy. It does this through lobbying, legal actions and lawsuits, information provision and campaigns for the general public.

882. The Freedom community (Freedom B.V.) is committed to a free, open and accessible internet. It was founded in 2019 by former XS4ALL employees and combines its technical expertise with an ethical view on privacy.

883. Qyi Foundation is a Dutch non-profit organization, aimed at giving consumers control over their own (personal) data. Qyi Foundation has developed an agreement system that provides access to, management and sharing of their own data by consumers. The Foundation has not been idle and carried out various activities (margin number 870 from which it also follows that it represents the interests of the Victims.

884. The Foundation will also explain below that they have sufficient expertise and experience to represent the interests of the Victims. Also, it follows from this that the Foundation is sufficiently representative to represent the interests of the Victims.

8.4.2 (ii) The requirements of Article 3:305a(2)(a) to (e) of the Dutch Civil Code

8.4.2.1 Introduction

885. Pursuant to the new Art. 3:305a(2)(a) to (e) of the Dutch Civil Code, the interests of the persons for whose benefit the judicial proceedings are brought, are sufficiently guaranteed if the legal person:

a. has a supervisory body;

b. provides appropriate and effective mechanisms for participation or representation in the decision-making of the individuals, to protect whose interests the judicial proceedings extend;

c. has sufficient funds to cover the cost of bringing judicial proceedings;

d. has a generally accessible Internet page showing:

- the Articles of Association
- the governance structure
- an outline of the last adopted annual report of the supervisory body about the monitoring it has carried out
- the last adopted management report
- the remuneration of directors and members of the supervisory body

[587] For an overview of the activities of Bits of Freedom, see: https://www.bitsoffreedom.nl/dossiers/europese-privacyregels/.

- the aims and methods of the legal person
- an overview of the state of affairs in ongoing proceedings and if a contribution is required of individuals, to protect whose interests the judicial proceedings extend
- an insight into the calculation of the contribution and an overview the manner in which individuals, the protection of whose interests the judicial proceedings extend, can join the legal person and the manner in which they can terminate this affiliation.

e. has sufficient experience and expertise in the setting up and conduct of judicial proceedings.

886. Two central questions are important for this:[588] (i) to what extent do the Victims ultimately benefit from the collective action, if the claim is awarded? and (ii) to what extent can it be trusted that the interest group has sufficient knowledge and competence to conduct the proceedings?

887. The Foundation is organised such that the Victims will actually benefit from this action. The Foundation does not ask for any compensation from the Victims. If the Foundation's claims are awarded, the Foundation pays a fee only to the Funder, because the Funder funds these proceedings.[589] In addition, the Foundation has ensured that it has sufficient in-house knowledge and competence to conduct the proceedings.[590] The Foundation will discuss that in more detail below.

8.4.2.2 Composition of the Supervisory Board

888. Through a careful selection process, highly competent people have committed themselves to the Foundation. The Foundation is pleased that it can rely on the following people.

Board

889. The Board consists of the following three Board members: Mr Hugo Hollander, Mr Joris van Hoboken and Ms Annelies van der Ploeg.

890. Mr Hugo Hollander is the chairman of the Board. Mr. Hollander is a chartered accountant and partner of his own social accounting firm Share Impact Accountants. Until 2016, he was audit partner at EY and, besides general accountant, he was also responsible for sustainability accounting. He is also active as a commissioner and supervisor of several social organisations. He is also a jury member of the Sustainability Award of the King Willem I Foundation. He is co-author of two management books: Guidance on inspired leadership (2014) and sustainability is history (2017).[591]

891. Mr Van Hoboken (general member) is a professor at the Free University of Brussels and senior university lecturer at the Institute for Information Law (IViR) at the Faculty of Law of the University of Amsterdam. Mr. Van Hoboken operates at the intersection of the protection of fundamental rights (data privacy, freedom of expression, non-discrimination) and the regulation of Internet services and platforms, and is a specialist in European data protection,

[588] *Parliamentary Papers II,* 2011/12, 33 126, 3, p. 12-13.
[589] For the financial resources of the Foundation, see section 8.4.2.4 and for the external funding, section 8.4.3, Principle III. External funding.
[590] *Parliamentary Papers II,* 2011/12, 33 126, 3.
[591] https://theprivacycollective.nl/over-ons/.

algorithmic regulation and the regulation of online intermediaries. Mr Van Hoboken has spent years as chairman of the board of Bits of Freedom. [592]

892. Ms Van der Ploeg (general member) is a lawyer in (commercial) dispute resolution and a partner at the firm BarentsKrans in The Hague. [593]892. The Board consists, therefore, of expert people who have the specific experience and financial and legal expertise that is necessary for safeguarding the interests of the Foundation's support base.

Supervisory Board

894. The Supervisory Board comprises (currently) the following two members: Ms Tonkens-Gerkema and Ms Toxopeus. At the time of the writ, there is a vacancy on the Supervisory Board, which will be filled in shortly.

895. Ms Tonkens-Gerkema is the former vice president and judge of the Court of Amsterdam. After her retirement, she served for several years as a deputy judge at the Court of Appeal of Amsterdam. She is a committee member of the Committee that drew up a revised version of the Dutch Claim Code in 2019 and thus has extensive expertise in the field of class actions. She is also a member of the Supervisory Board of the OCA (Research Collective Actions) foundation and the Elco Foundation. From 2001 to 2008 she was Chairman of the Dutch Association for the Judiciary. She is still working as an independent arbitrator. She is also chairman of the Committee of the Netherlands Arbitration Institute that decides on requests to challenge NAI arbitrators.[594]

896. Ms. Toxopeus is a professional with over twenty years of experience gained in both the accounting domain and the legal profession. Since 2012, she is affiliated as a partner at Hermes-Advisory. She is considered an expert in the execution and management of fraud investigations, in which she is dedicated to the calculation of financial loss and giving support in legal disputes. In her early career, Ms. Toxopeus worked at PwC, where in 1998 she joined the international audit practice of the Big Four firm. Later she worked at PwC in the forensic branch, where her focus was, among other things, on the implementation of fraud investigation. Following her time at PwC, Ms. Toxopeus also worked for more than five years at the law firm NautaDutilh, where she was appointed Corporate Litigation Advisor. Since 2014, she is lecturer and programme manager at the Erasmus School of Accounting & Assurance, where she has also designed the FFD training (Financial Forensic Expert). In her new role as a partner at BDO, Ms. Toxopeus will manage the Forensics & Litigation Support practice, part of Risk Advisory Services. [595] Ms Toxopeus was nominated by the Funder.

897. Therefore the Supervisory Board also consists of expert persons. The Supervisory Board has (already, even while there is a vacancy) the specific experience and financial and legal expertise that is necessary for safeguarding the interests of the Foundation's support base. With the Supervisory Board, the Foundation has internal supervision of the management and thus complies with Article 3:305a(2)(a) of the Dutch Civil Code.[596]

[592] https://theprivacycollective.nl/over-ons/.
[593] https://theprivacycollective.nl/over-ons/.
[594] https://theprivacycollective.nl/over-ons/.
[595] https://theprivacycollective.nl/over-ons/
[596] *Parliamentary Papers II,* 2016/17, 34608, 3, p. 19; Principle VI of the Claim Code 2019.

8.4.2.3 Participation and representation in decision-making

898. Article 3:305a(2)(b) of the Dutch Civil Code, requires an interest group that brings collective action to have effective and appropriate mechanisms for the participation or representation in the decision-making of the people for whom the judicial proceedings are being brought. Interest groups are free to determine how they implement this. When an interest group is arranged in accordance with the Claim Code, it can be assumed that it has complied with this requirement.[597]

899. In Section 8.4.3, the Foundation will Illustrate that it is arranged in accordance with the Claim Code. In addition, the Foundation will consult with the Victims if it considers supporting a settlement with Oracle and/or Salesforce. The Foundation will determine the exact manner in which it does this on the basis of the scope of that settlement and the most suitable manner at that time of involving the Victims in this process. The Foundation thus complies with Article 3:305a(2)(b) of the Dutch Civil Code.

8.4.2.4 The Foundation has sufficient financial resources

900. Article 3:305a(2)(c) of the Dutch Civil Code gives the court the opportunity to marginally assess whether the legal person who brings a collective action has sufficient resources to conduct the proceedings, and, moreover, where the interest group has sufficient control of the claim (in consultation with the support base).[598] It is sufficient that a legal person may indicate that, at the time of review, he has (or can have) sufficient funds to conduct the proceedings. The assessment is marginal. It is not necessary that the other party gains an insight into the funding agreement.[599]

901. The Foundation has concluded a funding agreement (the "**Funding Agreement**") with Innsworth Capital Limited (the "**Funder**"). Through its affiliated (project) companies the Funder has extensive experience in funding class actions and mass tort cases. The Foundation can make use of that experience.

902. In the Funding Agreement, the Foundation and the Funder acknowledge that the Victims in this case should have certainty about the funding of these proceedings. The Funder has therefore made ample funds available to the Foundation in order to conduct the proceedings in the first instance. This will also meet the requirement of Article 3:305a(2)(c) of the Dutch Civil Code.

903. In the discussion of Principle III of the Claim Code, the Foundation will illustrate the external funding in more detail.

8.4.2.5 The Foundation has an accessible website

904. The Foundation maintains a website, https://theprivacycollective.nl, which has and will have information such as the Articles of the Foundation, the Foundation's governance structure, an outline of the last adopted annual accounts of the supervisory body about the monitoring it

[597] *Parliamentary Papers II,* 2016/17, 34608, 3, p. 20.
[598] *Parliamentary Papers II,* 2016/17, 34608, 3, p. 11-12, 20.
[599] HR 20 December 2002, ECLI:NL:PHR:2002:AE3350 (*Lightning Casino/Antilles*); *Parliamentary Papers II* 2017/18, 34608, 6, p. 11-12.

has carried out, the recently adopted management report, the remuneration of directors and members of the Supervisory Board, the aims and methods of the Foundation, as soon as relevant an overview of the state of affairs in ongoing legal proceedings and a summary of how people, the protection of whose interests the judicial proceedings extend, can join the legal person and the manner in which they can terminate this affiliation.

905. The Foundation (also) maintains a comprehensive campaign website: https://theprivacycollective.eu/nl/ (margin number 870). This campaign website contains additional information about its activities. Various articles and studies are also published on the campaign website.

906. The Foundation thus complies with the conditions laid down in Article 3:305a(2)(d) of the Dutch Civil Code.

8.4.2.6 Experience and expertise

907. The Foundation has the experience and expertise required to bring these collective action proceedings. It has this expertise in-house, because its Board members and members of the Supervisory Board have the necessary expertise and competence, as explained in more detail in Section 8.4.2.2 above. They have extensive experience in the field of collective action, legal experience and expertise in the field of data protection and the protection of fundamental rights, knowledge and skills of digital commerce and the required financial expertise and experience.

908. In addition, the Foundation uses external specialists to investigate the practices of Oracle and Salesforce and the techniques they employ. The specialists specialize, inter alia, in technical research into privacy aspects when using, for example, cookies and similar technologies.

909. The Foundation is also supported by the interest groups Bits of Freedom, Privacy First, Freedom Internet B.V. and Qiy Foundation (margin number 870). These organisations have years of experience and expertise in this field.

8.4.3 The Foundation meets the requirements of the Claim Code

910. For this purpose, the Foundation has explained that the interests of the Victims it represents are sufficiently safeguarded. This is reinforced because the Foundation not only focuses on the demands of the legislator, which has codified a number of requirements of the Claim Code, but it was also inspired by the other requirements of the Claim Code. Based on the classification of the Claim Code 2019 and the corresponding statutory provisions, the Foundation will explain below how it has incorporated the terms or guidelines in question into its structure and governance.

Principle I – Compliance with and enforcement of the code

911. The Foundation's Board and the Supervisory Board are responsible for compliance with the Claim Code and the governance structure. They are accountable for this because they have worked out the main outlines of its governance on the Foundation's website https://theprivacycollective.nl. It has published a Claim Code document on the website (**Exhibit** 31). In the document, the Foundation explains the extent to which it follows the

provisions contained in the Claim Code and, if not, why and to what extent it derogates from them.[600] The information will remain on the website as long as the Foundation is active. Thus the Foundation complies with Principle I, elaboration 1.

912. Article 17(3) of the Foundation's Articles of Association states that any proposed change in the Foundation's governance structure and in the compliance with the Claim Code shall be submitted to the Foundation's Supervisory Board for discussion under a separate item of agenda. This is in accordance with Principle I, elaboration 3.

Principle II. – The Foundation has no profit motive

913. The Foundation was not set up to make money. This also had an impact on the organisation of the Foundation. The Foundation's objective shows that it has no profit motive.[601] No director, member of the Supervisory Board or the Funder may have access to the Foundation's funds, other than in the implementation of the Foundation's budget (Article 3(4) of the Articles of Association). In addition, the Foundation does not charge compensation to the Victims, which also significantly reduces the risk of improper use of the Foundation's funds.

914. The Foundation has chosen to have the current proceedings funded by the Funder. The Funder does, however, seek a profit on its funding. As a result, the Foundation will have to take into account the interests of the Funder within certain limits. On the other hand, the advantage for the Victims is that they do not have to pre-finance the proceedings, they do not bear a risk of legal costs, and they can use the expertise and resources of the Funder. A reasonable remuneration for borrowed capital is not a prohibited profit motive of the Foundation under Principle II, elaboration 2, and is therefore in accordance with the Claim Code.

915. Finally, Article 21(3) of the Articles of Association stipulates that if the Board passes a resolution to dissolve the organisation, the allocation of the liquidation balance will also be determined. This allocation must be as far as possible in accordance with the objective of the Foundation and benefit the support base of the Foundation, or a public non-profit organisation with a similar objective as the Foundation. The resolution for dissolution and the allocation of the liquidation balance, which is part of it, requires the prior written approval of the Supervisory Board. In other cases of dissolution, the allocation of the liquidation balance is determined by the liquidators. This complies with Principle II, elaboration 3.

Principle III. – External funding

916. The Foundation's Board has investigated the capitalisation, track record and the reputation of the Funder. In this context, it received further explanations and commitments from the Funder and its founders on request. The Foundation was advised and supported in this respect by its own lawyers. With regard to the present proceedings, the Foundation has agreed a budget with the Funder, to which it is obliged to comply under that agreement.

917. In Article 18 of the Articles of Association, the Foundation has indicated that it ensures that individual Board members and members of the Supervisory Board, as well as the lawyer or other service providers engaged by the Foundation, are self-sufficient and independent with respect to the Funder, and that the Funder is independent of the other party in the collective

[600] See also Article 17 of the Foundation's Articles.
[601] See Article 3 of the Foundation's Articles (**Exhibit 2**).

action. This article also states that the Funding Agreement provides for such an arrangement. Finally, it is stipulated that the Board ensures that the funding conditions (including the size and methodology of the remuneration to be agreed) do not reasonably conflict with the collective interest of the Victims.

918. The elaborations of Principle III of the Claim Code have been given the following place within the Funding Agreement:

1. Elaboration 2: The Funding Agreement is entered into in writing and comprises a choice for Dutch law and the jurisdiction of the Dutch courts.

2. Elaboration 3: Control of the process and settlement strategy rests solely with the Foundation. The Foundation and the Funder have however made agreements on the consultation of the Funder and continuous provision of information.

3. Elaboration 4: The Foundation has had laid down in its lawyers' engagement letters that the lawyers will act exclusively for and for the benefit of the Foundation. For as long as they work for the Foundation, the lawyers do not accept any assignments from the Funder.

4. Elaboration 5: The Funding Agreement provides for an appropriate arrangement as to the sharing of information with the Funder of the information belonging to the interest group. This arrangement defines what information the Funder may access.

5. Elaboration 6: The Funding Agreement arranges funding that enables the Foundation, as an exclusive representative, to pay the entire first instance.

6. Elaboration 7: The Foundation's website states that there is a Funder, (ii) the identity and residence of the external Funder and (iii) the systematic outline of the fee(s) and services agreed with the Funder. It also states the remuneration percentage payable to the Funder:

> "*The Foundation is funded by Innsworth Capital Limited, a litigation Funder based in Jersey. Depending on the extent of success the commission of the litigation Funder will be differentiated at 25%, 15% and 10% of the compensation awarded. The percentage thus decreases as the amount of the compensation gained increases. The final compensation will be reasonable and adequate considering the risks taken by the litigation Funder. In exchange for this, the Victims can join the Foundation free of charge and benefit from its activities. The commission payable to the litigation funder will reduce the amount available to the Victims, unless the Foundation's costs (including the commission that the litigation Funder has negotiated for funding and litigation risk) are included in the fees payable by Oracle and Salesforce.*"

7. Elaboration 8: The Funding Agreement states that the Foundation is authorised to provide further information to the court on the basis of an order to that effect. Insofar as the court sees fit to do so, the Foundation asks the court expressly to consult this information in a manner such that Oracle and Salesforce have no access to this

information. Such access is undesirable. The judicial review should normally only be marginal.[602]

Principle IV. – Independence and avoidance of conflicts of interest

919. The Board of the Foundation is composed such that the members can operate independently and critically relative to one another, the Supervisory Board, the Funder and the Victims at the Foundation. This is also included in Article 4(5) and Article 14 of the Articles of Association of the Foundation.

920. It should be noted in this context that the Funder has appointed Ms Toxopeus, member of the Supervisory Board, as its representative. The Foundation has also published this on its website. The appointment of Ms Toxopeus by the Funder is explicitly authorised by Principle VII, elaboration 3.

921. The Foundation has not entered into an agreement with any of the directors or the members of the Supervisory Board, except for the appointment letters containing the conditions for the exercise of their duties on behalf of the Foundation.

Principle V. – The composition, role and functioning of the Board

922. The Foundation's Board has a balanced composition. The Board consists of Mr Hugo Hollander, Mr Joris van Hoboken and Ms Annelies van der Ploeg. As has already been explained in section 8.4.2.2 "Composition of the Board and Supervisory Board", the Board also has, inter alia, the specific experience and legal and financial expertise that the Foundation requires in order to represent the Victims' interests adequately.[603] This is also in line with Article 4(5) of the Foundation's Articles of Association, which state that the Board is composed such that it has the specific expertise that is required for the adequate representation of the interests of the Victims.

923. The representative authority always rests with two of the three directors, as follows from Article 9 of the Articles of Association (Principle V, elaboration 5). All significant agreements to which the Foundation is a party, such as, for example, the Funding Agreement, are signed by two directors on behalf of the Foundation.

924. The Board also submits the balance sheet, statement of income, expenditure and budget for approval to the Supervisory Board (in accordance with Principle V, elaboration 6).

925. The Board regularly consults with members of the Supervisory Board. This is usually done via video conference. Minutes are made of the consultations. The Supervisory Board is also informed on a structural basis on relevant developments. The Board submits potentially far-reaching decisions to the Supervisory Board for approval. Article 5(4) of the Foundation's Articles of Association contains a list of resolutions subject to approval (in accordance with Principle V, elaboration 7). From this it follows that the consent of the Supervisory Board is required for the conclusion of a settlement agreement.

[602] See also *Parliamentary Papers II,* 2017/18, 34608, 6, p. 11-12.
[603] See also Article 4(6) and (7) of the Articles of the Foundation.

926. The Board also maintains a website, https://theprivacycollective.nl, on which detailed information is available (margin number 870). This fulfils Principle V, elaboration 8.

Principle VI. - Fees for directors

927. Article 4(8) of the Foundation's Articles states that the Supervisory Board may grant remuneration to the Board members. This is consistent with Principle VI, elaboration 1. The directors may not accept any compensation for their activities from any other than the Foundation or the Supervisory Board (Article 4(9) of the Foundation's Articles of Association, in accordance with Principle VI, elaboration 2).

928. The Foundation will report on the remuneration policy and payments to members of the Board in its annual report (Principle VI, elaboration 3). The main points of the remuneration policy can also be found on the Foundation's website, https://theprivacycollective.nl (Principle VI, elaboration 4).

Principle VII. – the Supervisory Board

929. The Supervisory Board consists of Ms Tonkens-Gerkema and Ms Inge Lisa Toxopeus. As has already been explained in section 8.4.2.2 "Composition of the Board and Supervisory Board", the Supervisory Board also has, inter alia, the specific experience and legal and financial expertise that the Foundation requires in order to represent the Victims' interests adequately (Principle VII, elaborations 4 and 5).

930. Ms. Toxopeus has been appointed by the Funder as the representative of the Funder. The Foundation has also published this on its website (Principle VII, elaboration 3).

931. The members of the Supervisory Board are independent of each other, the Board and with respect to the interests represented by the Foundation (Article 10(2) of the Articles of Association and Principle VII, elaboration 2). The members of the Supervisory Board can operate independently and critically (and do so as well). The Supervisory Board sees all requested documents and is provided with the necessary documents and information in a timely manner (Principle VII, elaboration 6).

932. The Supervisory Board meets regularly every year to discuss strategy and policy (Principle VII, elaboration 1).

933. Furthermore, the Supervisory Board may instruct an audit of the balance sheet and statement of income and expenditure by a chartered accountant, or other expert, appointed by the Supervisory Board (Article 16(3) of the Foundation's Articles of Association). This fulfils Principle VII, elaboration 7.

934. The Supervisory Board draws up an annual document containing an outline of its accountability for the monitoring it has carried out. This document is also published on the Foundation's website, https://theprivacycollective.nl. This also follows from Article 12(4) of the Articles of Association and is in accordance with Principle VII, elaboration 8.

935. Finally, on its website, the Foundation publishes the fixed expenses and fees for the members of the Supervisory Board (Article 5(6)(k) of the Foundation's Articles of Association and Principle VII, elaboration 9).

8.5 Additional eligibility requirements

8.5.1. Introduction

936. Article 3:305a(3) of the Dutch Civil Code contains a number of additional eligibility requirements for interest groups. The Foundation will explain below that it meets these requirements: the Board has no profit motive, the collective claims have a sufficiently close connection with the Dutch legal sphere, and the Foundation has invited Oracle and Salesforce for consultation, but the discussions held have not led to the desired result.

8.5.2 No profit motive

937. Article 3:305a(3)(a) stipulates that directors involved in the establishment of an interest group and their successors may have no direct or indirect profit motive, which is achieved through the interest group.

938. The Foundation has no profit motive (Article 3(3) of the Articles of Association). Neither do its directors have any profit motive. In the discussion of Principle II of the Claim Code, the Foundation has explained that its Board members, members of the Supervisory Board or the Funder cannot have access to the Foundation's funds, other than in the implementation of the Foundation's budget (Article 3(4) of the Articles of Association).

939. Article 21(3) of the Articles of Association also stipulates that the liquidation balance will be dealt with responsibly.[604]

8.5.3 Sufficiently close connection with the Dutch legal sphere

940. Pursuant to Article 3:305a(3)(b) of the Dutch Civil Code, the collective claim must have a sufficiently close connection with the Dutch legal sphere. The Foundation should make it sufficiently plausible that:

(i) the majority of the people, the protection of whose interests the judicial proceedings extend, have their habitual residence in the Netherlands; or

(ii) the one against whom the judicial proceedings are directed, is domiciled in the Netherlands and additional circumstances indicate sufficient connection with the Dutch legal sphere; or

(iii) the event or events to which the judicial proceedings pertain take place, or have taken place, in the Netherlands.

941. At (i): in these proceedings, the Foundation represents the interests of Dutch Internet users who have their habitual residence in the Netherlands. The support base can express its support for these proceedings through the campaign website.[605]

942. At (ii): Within the meaning of the GDPR, Oracle Nederland BV (defendant sub 1) and SFDC Netherlands BV (defendant sub 2) are establishments of Oracle and Salesforce, and are located

[604] See also Section. oabove: Principle II. – The Foundation has no profit motive; *Parliamentary Papers II*, 2016/17, 34608, 3, p. 21.
[605] For this, see section 6.2.

in Netherlands. The fact that Oracle Corporation (defendant sub 3), Oracle America Inc. (defendant sub 4) and Salesforce.com Inc. (defendant sub 5) are located in America does not alter the admissibility of the Foundation regarding these parties. In addition, violations of the privacy rights and the infringements of personal data have occurred in the Netherlands.

943. At (iii): this requirement refers to the place where the events actually occurred. It is not a reference to the place where the direct damage was suffered.[606] The violation of privacy rights and the infringements of personal data of Dutch Internet users, the Victims, have occurred in the Netherlands.

944. From the foregoing it follows that the collective claims in these proceedings have a sufficiently close connection with the Dutch legal sphere.

8.5.4. The Foundation has invited Oracle and Salesforce for consultations

945. By registered letter of 03 June 2020, the Foundation has held both Oracle (**Exhibit 3**) and Salesforce (**Exhibit 4**) liable for the damages suffered by its support base as a result of violations of the right to protection of privacy and the right to protection of personal data. The Foundation has thereby invited Oracle and Salesforce to consult with the Foundation for the granting of a reasonable compensation for the damages suffered by its support base.

946. Consultations were held with Oracle on 07 July 2020. The consultations have not resulted in the parties coming closer together.

947. Consultations with Salesforce took place on 03 July 2020. Neither has that consultation led to a solution.

948. Thus, the Foundation has also met the consultation requirement of Article 3:305a(3)(c) of the Dutch Civil Code.

8.6 Conclusion

949. The requirements of Article 3:305a of the Dutch Civil Code to bring collective action have definitely been met.

9. JURISDICTION AND APPLICABLE LAW

9.1. Jurisdiction

950. The Court has jurisdiction over the present dispute for the following reasons.

9.1.1 Primary: 79(2) of the GDPR

951. The GDPR contains its own rules on jurisdiction in Article 79. The second paragraph reads:

> *"Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller*

[606] *Parliamentary Papers II,* 2016/17, 34608, 3, p. 28.

> *or processor is a public authority of a Member State acting in the exercise of its public powers."*

952. The Dutch court thus has jurisdiction if the controller or the processor against which the claim is made has an establishment in the Netherlands, *or* the data subject has his habitual residence in the Netherlands.

953. Recital 145 of the GDPR clarifies that the plaintiff may choose himself where he brings the case:

> *"For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers."*

954. As explained in section 6.2, the majority of the people, the protection of whose interests the judicial proceedings extend, have their habitual residence in the Netherlands. The Foundation focuses in this case on the data subjects of which about 10 million have their habitual residence in the Netherlands (see margin number 0).

955. The foregoing means that under Article 79(2), the Court has jurisdiction with respect to this dispute.

9.1.2 In the alternative: Article 2 in conjunction with Article 7 of the Dutch Code of Civil Procedure

956. The Dutch court has jurisdiction in this case and the court has territorial jurisdiction to hear the claims against all Defendants. This follows from Article 7 of the Dutch Code of Civil Procedure ("**DCCP**") in conjunction with the rules of Dutch common international law of competence, namely DCCP Articles 1-13.

957. Now that Oracle Nederland BV and SFDC Netherlands BV are based in the Netherlands, it holds that the court has jurisdiction against Oracle Nederland BV and SFDC Netherlands BV under the general rule contained in DCCP Article 2.

958. Salesforce.com Inc., Oracle Corporation and Oracle America, Inc. are based in America. Therefore, the case against these defendants has an international character. Regulation (EU) No, 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (hereafter: "**Brussels I-bis Regulation**") does not apply to these defendants now they have no residence in the territory of a Member State of the European Union. Other international regulations in the area of jurisdiction do not apply in the present case. That means that the international jurisdiction of the court with respect to these defendants must also be assessed by reference to DCCP Articles 1-13.

959. The court also has jurisdiction under DCCP Article 7 with respect to these defendants. Between the claims brought against these defendants and the Dutch defendants, Oracle Nederland BV and SFDC Netherlands BV, there exists such a consistency that reasons of efficiency warrant a

joint hearing. In the case of separate hearings and sentencing, it should also be avoided that irreconcilable judgments are made in the cases.

9.2 Applicable law

960. The GDPR (see section 4.4.1) and the Tw (see section 4.4.2) apply to the actions of Oracle and Salesforce.

961. Now that both the Foundation [on the one hand] and Oracle Nederland BV and SFDC Netherlands BV are based in the Netherlands, Dutch law applies to the Foundation's claims against these defendants.

962. Dutch law also applies to the claims against the American defendants, Salesforce.com Inc., Oracle Corporation and Oracle America, Inc.

963. The claims against these defendants are not related to a contractual obligation, but to a non-contractual obligation, an unlawful act or species of tort. This means that in principle, the EU regulation No. 864/2007, on the law applicable to non-contractual obligations (hereafter: "**Rome II Regulation**"), is eligible for application.

964. A number of the claims, however, are connected in part with topics that are excluded from the material scope of the Rome II Regulation. Thus, non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation, are excluded (Article 1(2)(g) of the Rome II Regulation).[607]

965. In that case, the Rome II Regulation does not apply, unless under Article 10:159 of the Dutch Civil Code the Regulation applies mutatis mutandis to the commitments that in principle fall outside the scope of the Regulation.[608] Under Article 10:159 of the Dutch Civil Code, the Rome II Regulation applies mutatis mutandis to the claims against Salesforce.com Inc., Oracle Corporation and Oracle America, Inc., which would be excluded in principle from the scope. According to the general rule laid down in Article 4(1) of the Rome II Regulation, the law of the country where the damages occurred is applicable (lex loci damni), namely the Netherlands.[609] Dutch law is thus also applicable to the claims against the American defendants.

10. KNOWN DEFENCES AND REFUTATION

10.1 Oracle's defences

966. Oracle has, inter alia, by letter dated 18 June 2020 (**Exhibit 5**), defended itself as follows:

a. Oracle claims that the arguments of the Foundation are unfounded, because:

[607] Asser/Kramer & Verhagen , 10-III , 2015/984.
[608] Asser/Kramer & Verhagen , 10-III , 2015/975. defamation.
[609] Asser/Kramer & Verhagen , 10-III , 2015/977.

i. the Foundation would have a wrong understanding of the services supplied by Oracle and bases its findings on incorrect assumptions or misunderstandings about the Oracle services;[610]

ii. the Oracle services would not be "crucial" for the RTB process;[611]

iii. it complies with the requirements in the context of the GDPR and the Tw.[612]

In its letter, Oracle makes a distinction between its DMP-service and a service called "Audience Data Marketplace" ("**ADM**"). It claims that it should be regarded as a processor for its DMP service. According to Oracle, there are only "first-party cookies" that are placed by its customers.[613] Oracle would thereby not dictate or check what information its customers collect, nor would they use the data its customers collect for its own purposes.[614] Oracle believes that it therefore does not have to comply with the GDPR obligations that apply to controllers.[615] In section 4.4 we have explained why this assertion of Oracle is incorrect. It is Oracle that takes the initiative for the data processing, determines the means thereto and has the greatest commercial interest therein. Research shows that Oracle itself places the cookies (**Exhibit 16**). Moreover, Oracle itself acknowledges in its privacy documentation that it is a controller.

b. Oracle acknowledges in its letter that it is an (independent) controller with regard to the ADM service, which it describes as an "*optional cloud-based third-party data marketplace service offered to DMP customers*".[616] The distinction that Oracle tries to make here between its DMP and the ADM service does not, however, exist. The ADM service is an integral part of the DMP service of Oracle. Oracle itself endorses this in its commercial documentation. It describes its DMP on its website as follows:

> *"Oracle DMP (formerly BlueKai) is the industry's leading cloud-based big data platform that enables marketing organizations to personalize online, offline, and mobile marketing campaigns with richer and more-actionable information about targeted audiences."*[617]

If on Oracle's website the potential client clicks on "Request a Consultation" to ask for more information about the Oracle DMP, Oracle will state:

> *"With the Oracle DMP, marketers will:*
>
> *Access the industry's largest 3rd party data marketplace*
>
> *Gain a holistic view of your customers with 1st and 3rd party data*

[610] Oracle letter of 18 June, under 1 'Oracle's Services in the Netherlands', p 1.
[611] Oracle letter of 18 June 2020, under 2 'Oracle's DMP and ADM Services are not "crucial" to the RTB Process', p. 3.
[612] Oracle letter of 18 June 2020, under 3 'Oracle complies with the GDPR and DTA with respect to the ADM services', p. 3.
[613] Oracle letter of 18 June 2020, under 1.a.1 'Data Management Platform, p. 1.
[614] Ibid.
[615] Oracle letter of 18 June 2020, under 1.a.1 "Oracle is a processor for the DMP', p 2.
[616] Oracle letter of 18 June 2020, under 1.a.2 "Audience Data Marketplace' and 'Oracle is an independent controller for the ADM', p. 2.
[617] https://www.oracle.com/data-cloud/products/data-management-platform/, consulted on 23 April 2020.

Resolve disparate identities and deliver streamlined experiences

With the addition of Oracle OnRamp, extract the full value from your offline customer data with online audiences that deliver superior customer experiences and drive new customer growth"[618]

Oracle describes ADM therefore as an integral part of its DMP service. That is why it is therefore the controller for the total DMP service, including ADM.

c. Oracle further wrongly alleges that the Foundation claims that Oracle combines its DMP service with other services, such as AddThis. [619] It is alleged that it was decided in 2018 to discontinue the AddThis data collection in Europe. According to Oracle, the data collected with AddThis in areas outside the EU would not be combined or used for the ADM service in the Netherlands. Oracle does not specify in its letter, however, when in 2018 (before or after 25 May 2018), this decision was taken exactly, nor when and to what extent this decision has been implemented in practice. The Foundation assumes that all this did not take effect before 25 May 2018. Moreover it is striking that the AddThis buttons are still used and many Publishers assume that data is also collected with them. This is evident, for example, from the explanation about cookies from RTL, which manages RTL News (*rtlnieuws*) and weather forecasts (*Buienradar*).[620] AddThis is included here in the "List of Advertising and Behavioural Cookies". The link that is included here after "Oracle AddThis" does not work.

d. Oracle claims that the "third-party data" it receives for the ADM service from selected data providers in the EU consists of cookie data, specific device identifiers such as IP addresses, and "interest segments".[621] Within the EU, Oracle would receive no direct identifiers such as name, surname, email address, postal address or telephone number. Even if Oracle would only process the above-mentioned data, which the Foundation disputes, there is still the processing of personal data for which consent is required. After all, cookie data, device indicators, IP addresses and "interest segments" qualify as personal data within the meaning of the GDPR (see section 4.3.1)) and Oracle cannot invoke another basis (see section 4.6.2.1). Oracle also claims that it does not collect, process or enrich the data sets with offline data from data subjects within the EU. That is difficult to understand, now that Oracle states in its Dutch privacy documentation that they collect both offline and online information about data subjects, including information derived from publicly available sources or external data providers (see section 3.2.4). Moreover, its privacy documentation states that the offline information about data subjects is retained for up to five years if it was collected in the EU/EEA.

e. In this regard, Oracle claims that it has designed a "robust due diligence programme" for suppliers of data.[622] Oracle would use this to carefully examine whether these parties have met the GDPR. From its own information, however, it follows that ShareThis is

[618] https://go.oracle.com/LP=90408, consulted on 21 July 2020.
[619] Oracle letter of 18 June 2020, under 1.b 'Incorrect allegations regarding the DMP and ADM services', p. 2.
[620] https://privacy.rtl.nl/uitleg-over-cookies
[621] Oracle letter of 18 June 2020, under 1.b 'Incorrect allegations regarding the DMP and ADM services', p. 2.
[622] Oracle letter of 18 June 2020, under 3 'Oracle complies with the GDPR and DTA with respect to the ADM services', p. 4.

one of the suppliers which has come through the selection.[623] As research shows, ShareThis is a party that collects data in an opaque manner on a large scale (see among others margin number 422 et seq.). It is impossible to claim adequate consent for this.[624]

f. Oracle also claims that its DMP activities meet the requirements of consent[625], transparency[626] and data minimisation[627]. In section 4.6.1 up to and including 4.6.4 it has been explained in detail that this is not the case.

g. In the discussion that took place on 07 July 2020, Oracle has further stated that the article published by TechCrunch[628] about its data breach is unfounded, without indicating what is incorrect about the facts mentioned in the article.

10.2 Salesforce's defences

967. Salesforce gave no substantive reply in its letter of 17 June 2020.[629] Salesforce only states that it disagrees with the conclusion of the Foundation that Salesforce violates the GDPR and Tw regarding its DMP service. Salesforce claims that this conclusion would be based on a number of misconceptions and false assumptions regarding the DMP of Salesforce and the data processing in the context of DMP. Salesforce says that its DMP does not work like "most other DMPs".[630] It is unclear to the Foundation what distinguishes Salesforce from other DMPs.

[623] http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf consulted on 23 April 2020.
[624].The Irish Times, *Data from HSE website users 'leaked to commercial actors',* 18 March 2019, to be consulted via: https://www.irishtimes.com/business/technology/data-from-hse-website-users-leaked-to-commercial-actors-1.3829547
[625] Oracle letter of 18 June 2020, under 3.a 'Oracle's ADM service is lawful and based on consent', p. 4.
[626] Oracle letter of 18 June 2020, under 3.b 'Oracle is transparent about its ADM processing activities', p. 5-6.
[627] Oracle letter of 18 June 2020, under 3.c 'Oracle's processing activities are fair, necessary, and proportionate', p. 7.
[628] Techcrunch, *Oracle's BlueKai tracks you across the web. That data spilled online',* 19 June 2020, to be consulted via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (see **Exhibit 12**).
[629] Salesforce letter of 17 June 2020.
[630] Salesforce letter of 17 June 2020, p. 2, paragraph 1.

11. RELIEF SOUGHT

REASONS WHY

The Foundation requests the Court to rule as follows, as far as possible enforceable:

Claim I: exclusive representative

I. To appoint the Foundation as the exclusive representative within the meaning of Article 1018e(1) of the Dutch Civil Code;

Claim II: definition of narrowly defined group

II. To determine that this collective action concerns the following group of natural persons in the sense of Article 1018d of the Dutch Code of Civil Procedure :

a. The group of natural persons who have been put at a disadvantage by Oracle Nederland BV, Oracle Corporation and Oracle America, Inc. (hereinafter collectively 'Oracle') (hereinafter the 'Oracle Group') and who consist of:

i. all natural persons

ii. who have, or have had, one or more computers with Internet access, or other peripherals within the meaning of the Telecommunications Act, in use, and

iii. on which a cookie with the name '**bku**' is placed, or has been placed,

iv. at a time or during a period in which they lived or stayed in the Netherlands, after the entry into force of the GDPR in this case; and

b. The group of natural persons who have been disadvantaged by SFDC Nederland BV and Salesforce.com, Inc. (hereinafter collectively 'Salesforce') (hereinafter the 'Salesforce Group') and who consist of:

i. all natural persons,

ii. who have, or have had, one or more computers with Internet access, or other peripherals within the meaning of the Telecommunications Act, in use, and

iii. on which a cookie with the name '**__kuid__**' is placed, or has been placed,

iv. at a time or during a period in which they lived or stayed in the Netherlands, after the GDPR became applicable in this case.

Claim III: opt-out possibility

III. To determine that:

a. each member of the Oracle Group and/or Salesforce Group residing or domiciled in the Netherlands for a period of three months after the notice referred to within the meaning of Article 1018f(3) of the Dutch Code of Civil Procedure of the decision to designate the exclusive representative, will have the opportunity to notify the Registry

of the Court in writing of the withdrawal of the defence of their interests in this collective action;

b. each member of the Oracle Group and/or Salesforce Group not residing in the Netherlands or having its domicile there for a period of six months after the notice referred to within the meaning of Article 1018f(3) of the Dutch Code of Civil Procedure of the decision to designate the exclusive representative, will have the opportunity to notify the Registry in writing of the acceptance of the defence of their interests in this collective claim;

Claim IV: declaratory judgement concerning liability

IV. To declare it law that:

a. for reasons set out in the body of this Writ Oracle and Salesforce are acting in contravention of the fundamental rights set out in the body of this Writ, the GDPR and the Dutch Telecommunication Act, and

b. each of Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. and Salesforce.com, Inc. are jointly and severally liable towards each member of the Oracle Group and the Salesforce Group so that if one of them has paid the others will be discharged to that extent, under Article 82 of the GDPR and/or Article 6:162 of the Dutch Civil Code, at any rate Article 6:212 of this Code for the damage suffered and to be suffered by each of those members;

at any rate that

a. Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc. are jointly and severally liable towards each member of the Oracle Group, so that if one of them has paid the other will be discharged to that extent under Article 82 of the GDPR and/or Article 6:162 of the Dutch Civil Code, at any rate Article 6:212 of the Dutch Civil Code for damages suffered and to be suffered by each of those members, and

b. SFDC Netherlands B.V. and Salesforce.com, Inc., are jointly and severally liable towards each member of the Salesforce Group for the damage suffered and still to be suffered, pursuant to Article 82 of the GDPR and/or Article 6:162 of the Dutch Civil Code, at any rate Article 6:212 of this Code, so that if one of them has paid the other will be discharged to that extent.

Claim V: order to payment of compensation with regard to the processing of personal data

V. Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc, SFDC Netherlands B.V. and Salesforce.com, Inc, are ordered jointly and severally to compensate the (immaterial and material) damage, so that if one of them has paid the other will be discharged to that extent, whether or not estimated under Article 6:104 of the Dutch Civil Code,

a. for the entire Oracle Group in total amounting to **€ 5 billion** and for the entire Salesforce Group amounting to **€5 billion**, all this to be increased by the statutory interest from the date of passing judgement, until the date of full settlement;

At any rate

b. **<u>€500 per person</u> in the Oracle Group** if he or she has, or has had, one or more computers with Internet access, or other peripherals, in use within the meaning of the Telecommunications Act, on which a cookie called 'bku' is placed or has been placed since the GDPR became effective in this case and **<u>€ 500 per person</u>** in the Salesforce Group if he or she has, or has had, one or more computers with Internet access, or other peripherals, in use within the meaning of the Telecommunications Act, on which a cookie called '_kuid_' is placed or has been placed since the GDPR became effective, all this to be increased by the statutory interest from the date of reaching a judgement, until the date of full settlement;

At any rate

c. To determine that the damages suffered and to be suffered by the Oracle Group and the Salesforce Group by virtue of that stated in the body of the writ shall be drawn up in more detail by the court and will be settled as prescribed by law;

<u>Claim VI: order to pay compensation with regard to Oracle's data breach</u>

VI. Each of Oracle Nederland B.V., Oracle Corporation and Oracle America, Inc. are jointly and severally ordered to compensate the (immaterial and material) damage so that if one of them has paid the other will be discharged to that extent, whether or not estimated on the basis of Article 6: 104 of the Dutch Civil Code,

a. **€100 per person** for each of the members of the Oracle Group and/or Salesforce Group whose data has been or may have been accessible during the security breach reported in June 2020 as indicated in the Writ, to be increased by the statutory interest from the date of the judgment to be rendered, until the day of payment in full;

At any rate

b. To determine that the damage suffered and still to be suffered in this respect by the Oracle Group and/or the Salesforce Group on account of the allegations set out in the body of the writ will be further assessed by the court in follow-up proceedings and will be settled as prescribed by law;

<u>Claim VII/VIII provision of information</u>

VII. That Oracle and Salesforce will list, in the form of an Excel table or comparable generally accepted file, within four weeks of the judgement to be passed in this matter, of:

a. All websites that can be visited from the Netherlands through which Oracle or Salesforce cookies are placed, and the dates and the period(s) during which that is (or has been) the case; and

b. All parties with which Oracle or Salesforce have exchanged data based on cookie identifiers and the dates and period(s) during which that is (or has been) the case; and

c. All data sources that Oracle or Salesforce have used to enrich profiles of members of the Oracle group and/or the Salesforce Group and the dates and the period(s) during which that is (or has been) the case, and

always insofar as it relates to the period from the GDPR becoming effective (25 May 2018) up to and including the date of serving judgement in this case,

And

VIII. To determine that:

That Oracle will list, in the form of an Excel table or comparable generally accepted file, within four weeks of passing judgment in this matter, the number of persons (possibly) living or staying in the Netherlands whose data has been (or may have been) accessed during the security breach, which was reported in June 2020 as specified in the writ, and the name and contact details of these individuals if and to the extent known, at least will take such technical provisions that everyone can verify for themselves freely and easily whether a breach has been made in connection with his or her personal data and on the nature, cause, scope and duration of the infringement and the data compromised;

IX. Under the provision that each of Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. and Salesforce.com.Inc. will be due a penalty if Oracle or Salesforce do not fully or timely meet any part of these convictions VI and VII, to the amount of € 1,000 per shortcoming, per day, with a maximum of € 50 million (each).

Claim X: costs of proceedings and fees

X. To order each of Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. and Salesforce.com, Inc. jointly and severally , so that insofar as the one has paid, the other will be discharged to that extent,, :to compensate the Foundation for the following

a. The full costs of proceedings of the Foundation under Article 1018l of the Dutch Code of Civil Procedure, at least the actual costs of proceedings under Article 237 of the Dutch Code of Civil Procedure, all this plus the statutory interest from the date of passing judgment, until the date of full settlement; and

b. The full (extra-judicial) costs of the Foundation under Article 6:96 of the Dutch Civil Code, all this plus the statutory interest from the date of passing judgement, until the date of full settlement,

Which amounts a. and b. are jointly estimated to be € 10 million, at least to be budgeted in more detail; and

c. The full agreed fee to be paid by the Foundation to the Funder, under Article 6:96 of the Dutch Civil Code and Article 1018l(2) of the Dutch Code of Civil Procedure, as budgeted in more detail based on further information to be submitted by the Foundation;

Claim XI: method of settling collective damages

XI. To determine that:

a. Oracle and Salesforce will pay to the Foundation:

i. all amounts to be paid to the Foundation and the Oracle Group and the Salesforce Group on the basis of this petition, based on 10 million members of the Oracle Group and/or the Salesforce Group, and to stipulate that any part remaining 24 months after payment by Oracle and Salesforce, at least a term to be determined on an equitable basis by Your Court, will be allowed to be paid by the Foundation to one or more non-profit organisations to be designated by the Foundation that are active in the field of privacy protection,

ii. to be increased by an additional amount of **€ 15 million** at least an amount to be determined on an equitable basis that will seek to redeem the costs to be incurred by the Foundation in dividing the damages compensation among the members of the Oracle Group and/or the Salesforce Group (hereinafter: 'Additional Amount'), under the provision that if and to the extent that any portion remaining of the Additional Amount after completing the division among the members of the Oracle Group and Salesforce Group and all costs of the Foundation connected therewith have been redeemed, will be refunded to Oracle and Salesforce within 30 days; and

b. The Foundation will hire a professional claim handler of good repute and instruct them to take care of the payment of the appropriate division of the damages to be paid by Oracle and Salesforce to members of the Oracle Group and Salesforce Group, and

c. That the members of the Oracle Group and Salesforce Group wishing to qualify for compensation should agree to a binding advice procedure, for which a binding consultant will be designated by the Court after consultation with the parties, as detailed by the Foundation and to be approved by your court;

d. At any rate to design the collective settlement of claims in such a way as Your Court will consider advisable on the basis of the proposals for collective compensation of damages to be submitted by the Foundation and Oracle and Salesforce under Article 1018i of the Dutch Code of Civil Procedure;

The costs of this document are €100.89

This case is being handled by:
mr Chr. A. Alberdingk Thijm, *mr* F.M. Peters, *mr*. S.C. van Schaik, *mr*. M. Krekels
bureau Brandeis
Sophialaan 8, NL - 1075 BR Amsterdam
T: +31(0)20 7606 505 / F: +31(0)20 7 606 555
info@bureaubrandeis.com / bureaubrandeis.com

EXHIBITS OVERVIEW

Exhibit 1	Information Commissioner's Office, "Update report into AdTech and real time bidding" of 20 June 2019 – an investigation into the RTB market of the UK supervisory authority for data protection.
Exhibit 2	Deed of incorporation of Foundation The Privacy Collective dated 29 May 2020.
Exhibit 3	Letter of summons dated 3 June 2020 to Oracle.
Exhibit 4	Letter of summons dated 3 June 2020 to Salesforce.
Exhibit 5	Response letter of Oracle dated 18 June 2020.
Exhibit 6	Response letter of Salesforce dated 17 June 2020.
Exhibit 7	Web pages of Oracle about its DMP service.
Exhibit 8	Web pages of Salesforce about its DMP service.
Exhibit 9	Example of a bku cookie placed by Oracle's domain bluekai.com, which shows the same Cookie ID with which the internet user is followed on various websites.
Exhibit 10	Example of a _kuid_ cookie placed by Salesforce's domain krxd.net, which shows the same Cookie ID with which the internet user is followed on various websites.
Exhibit 11	Nu.nl logbook - overview of what happens in a few seconds in the background when the front page of www.nu.nl is loaded.
Exhibit 12	Article on the technology website TechCrunch of 19 June 2020 about a data breach at Oracle's DMP service. TechCrunch also describes the operation of Oracle's DMP.
Exhibit 13	"Create Audience Segments" page of the Oracle website of 22 July 2020 in which Oracle explains how to create audiences with the Oracle BlueKai DMP using, among other things, Oracle data and data from third parties.
Exhibit 14	"Segment Builder Guide" page of the Salesforce website of 22 July 2020 in which Salesforce explains how the Salesforce DMP service (Audience Studio) can be used to create target groups with, among other things, Salesforce data and data from third parties.
Exhibit 15	"Oracle Marketing Cloud Teams with Eyeota to Enhance Global Data Offering", news item of 19 January 2017 on the Oracle website in which it describes, among other things, that Oracle's BlueKai Marketplace (part of DMP) contains more than 30,000 data points from more than 2 billion consumers, obtained through more than 1500 data partners.
Exhibit 16	Investigation report from Dr. Bashir of 12 August 2020 into the presence of Oracle and Salesforce technology on popular Dutch websites. Dr. Bashir concludes, among

other things, that technology from Oracle and Salesforce is used on 41 of 100 selected popular Dutch websites and that both parties engage in cookie syncing with dozens of other parties.

Exhibit 17 Relevant parts of the Oracle 2019 Data Directory that describe Oracle's data partners. Due to the large size of the document, only the pages are submitted that refer to data partners that are available in the EU according to Oracle.

Exhibit 18 Overview of websites popular in the Netherlands on which cookies from Oracle and/or Salesforce have been found, including information about the method of provision of information and consent mechanism.

Exhibit 19 Web pages of Oracle from which it follows, among other things, that Oracle is also focusing its DMP service on the Dutch market.

Exhibit 20 Salesforce web pages from which it follows, among other things, that Salesforce also focuses its DMP service on the Dutch market and news item of 24 September 2018 in which various large media companies (partly) aimed at the Netherlands indicate that they use the Salesforce DMP.

Exhibit 21 Overview of data that Oracle claims to process about a Dutch internet user, including 11 pages of different data segments that Oracle processes about this person.

Exhibit 22 Privacy documentation of Oracle (part):

- **a** Privacy policy for Oracle Data Cloud (in Dutch)
- **b** Oracle AddThis Privacy Policy (in English)
- **c** Oracle Data Cloud Privacy Policy (in English), version after 11 June 2020
- **d** Oracle Data Cloud Privacy Policy (in English), version until 11 June 2020

Exhibit 23 Privacy documentation of Salesforce (part):

- **a** Dutch overview page of Salesforce privacy documentation: https://www.salesforce.com/nl/company/privacy/
- **b** Salesforce General Privacy Statement (in Dutch)
- **c** English overview page of Salesforce's privacy documentation: https://www.salesforce.com/eu/company/privacy/
- **d** Salesforce Audience Studio Privacy Policy (in English)
- **e** Salesforce Trust and Compliance page (in English): https://trust.salesforce.com/en/trust-and-compliance-documentation/audience-studio-and-data-studio/

f Audience Studio Notices and License Information (in English)

Exhibit 24 Oracle Online Data Agreement v120119 and Data Processing Agreement version 26 June 2019.

Exhibit 25 Salesforce Data Processing Addendum, version July 2020.

Exhibit 26 Extract from the Chambers of Commerce of Oracle Nederland B.V. dated 24 June 2020.

Exhibit 27 Extract from the Chambers of Commerce of SFDC Netherlands B.V. dated 20 May 2020.

Exhibit 28 Overview of 24-28 July 2020 of popular Dutch websites that incorrectly request permission to place cookies of Oracle and Salesforce.

Exhibit 29 W. Christl, "Corporate surveillance in everyday life – How Companies Collect, Combine, Analyse, Trade, and Use Personal Data on Billions" of June 2017 – a report on the AdTech market, including, inter alia, explanations of DMPs state and a case study of Oracle.

Exhibit 30 Oracle tool with which internet users could deregister and/or have their data deleted.

Exhibit 31 Claim Code Compliance Document of Foundation The Privacy Collective, August 2020.