SPIRIT LEGAL®

Spirit Legal / Neumarkt 16-18 / 04109 Leipzig / Germany

Empfänger
Hamburg District Court
Sievekingplatz 1
20355 Hamburg

Spirit Legal Fuhrmann Hense
Partnerschaft von Rechtsanwälten
Neumarkt 16-18
D-04109 Leipzig
Germany

Tel.: +49 (0) 341 / 39 29 78 90
Fax: +49 (0) 341 / 39 29 78 99
E-Mail: info@spiritlegal.com
Web: www.spiritlegal.com

AG Leipzig
Partnerschaftsregister No. 243

AZ: 21/181/PHE/THB/ENK/CSC

Bearbeiter: Attorney Peter Hense, Attorney Tilman Herbrich and Attorney Elisabeth Niekrenz

Ihr Zeichen:

Ort, Datum: Leipzig, 15.04.2021

Lawsuit

by **Dr Johnny Ryan**, Irish Council of Civil Liberties, Unit 11, First Floor, 34 Usher's Quai, Dublin 8, D08 DCW9

- Plaintiff -

Litigation Counsel: Spirit Legal Fuhrmann Hense Partnership of Lawyers Neumarkt 16-18, 04109 Leipzig

1. **IAB Technology Laboratory, Inc.** , 116 East 27th Street 7th Floor, New York, NY 10016, USA, represented by vonwersch Digital Strategies GmbH, Grindelhof 69, 20146 Hamburg, Germany, represented by Oliver von Wersch, Managing Director.

- Defendant 1 -

2. **Xandr, Inc. ,** 28 West 23th Street, Fl. 4, New York, NY 10010, USA, represented by App Nexus Germany GmbH, Große Elbstraße 43, 22767 Hamburg, Germany, represented by Managing Directors Charles Brian O'Kelley, Michael Rubinstein, and Michiel Nolet.

- Defendant 2 -

3. **OnlineMarketing.de GmbH**, Ludwig-Erhard-Straße 14, 20459 Hamburg, Germany, represented by the Managing Director Marc Stahlmann

- Defendant 3 -

because of: **Data breaches**

Amount in dispute (preliminary): **EUR 10,000.00**

In the name of and on behalf of the plaintiff, we bring this action and will request at the hearing:

The defendants are ordered to avoid a fine to be set by the court for the case of infringement - in lieu of imprisonment - or imprisonment for up to six months (fine in individual cases not exceeding EUR 250,000.00, imprisonment for a total of not more than two years), to be enforced on their legal representatives,

to refrain from,

1. ***processing personal data of the plaintiff without appropriate security measures in accordance with art. 32 of the GDPR,***

   if this is done, as set out in Annex K 1;

2. ***processing personal data of the plaintiff without providing the plaintiff in a transparent and comprehensible and easily accessible form with the obligatory information under data protection law pursuant to art. 12 para. 1, 13 and 26 para. 2 sentence 2 GDPR,***

if this is done as shown in Annex K 2;

3. *processing the plaintiff's personal data without a legal basis,*

   if this is done, **as set out in Annex K 3***;*

4. *transferring personal data of the plaintiff to the United States without*
   a. *an adequacy decision pursuant to art. 45 GDPR,*
   b. *appropriate safeguards in accordance with art. 46 of the GDPR, or*
   c. *an exception in accordance with art. 49 GDPR.*

In the event that the written preliminary proceedings are ordered, we immediately request the

Issuance of a default judgment pursuant to section 331 Zivilprozessordnung (ZPO, Code of Civil Procedure) if the defendants do not indicate their willingness to defend in due time.

TABLE OF CONTENTS

JUSTIFICATION

A. Facts

The plaintiff objects to the processing of his personal data in the context of the sending of personalised online advertising. Through the challenged system Real Time Bidding (RTB), extensive information about the private online behaviour of people, including the plaintiff, is sent to thousands of companies. Real Time Bidding involves automated auctions for the advertising spaces on a website while that occur in real time as it is loading.

Users can thus be tracked in their user behaviour.

The rules of Real Time Bidding are defined worldwide by technical standards called “OpenRTB”, “AdCOM”, “Content Taxonomy” and “Audience Taxonomy”.

The OpenRTB protocol generated €6.7 billion in revenue in Europe in 2019 [IAB Europe, A.I.S.B.L., Programmatic Advertising spend in Europe 2019, 01.10.2020, available at: https://iabeurope.eu/wp-content/uploads/2020/10/Programmatic-Market-Advertising-Spend-2019-Report.pdf, last accessed 07.04.2021].

The action is directed against the subsidiary organisation of a trade association of the online advertising industry which, by providing the technical standards, significantly coordinates, organises, enables and encourages the challenged processes (1st defendant), against a company which operates a platform for the purchase and sale of online advertising space (2nd defendant), and against the operator of an online medium on whose website corresponding technologies are used (3rd defendant).

Real Time Bidding violates applicable data protection law millions of times every day. Even one of the inventors of Real Time Bidding and former managing director of the 2nd defendant, Brian O'Kelley, assumes that the technology is not compatible with the GDPR [*Schiff*, RTB RIP? The Writing Could Be On The Wall For Real-Time Bidding In Europe, Ad Exchanger, Aug. 06, 2019, available at: https://www.adexchanger.com/privacy/rtb-rip-the-writing-could-be-on-the-wall-for-real-time-bidding-in-europe/, last accessed on Apr. 01, 2021; Itega, RTB inventor says today's ad-tech is dead, IAB can't help, and it's time to help publishers build atop privacy, available at: https://itega.org/2020/07/10/privacy-beat-who-to-believe-will-big-business-be-helped-or-hurt-by-california-privacy-ballot-initiative-check-in-10-days/, last accessed on Apr. 01, 2021].

A class action lawsuit was filed in the U.S. in May of this year against Google's Real Time Biding system [*Davis*, Google Hit With Privacy Suit Over Real-Time Bidding, Media Post, Mar. 29, 2021, available at: https://www.mediapost.com/publications/article/361833/google-hit-with-privacy-suit-over-real-time-biddin.html, last accessed Apr. 06, 2021].

I. The parties

1. The plaintiff

The plaintiff is an Irish citizen and a Senior Fellow of the Irish Council for Civil Liberties, which has been involved in the protection of fundamental rights for 45 years. He has previously worked in advertising technology, the media industry and for a company which operates a web browser. He has written two books on Internet technologies. The plaintiff has extensive insight into how Real Time Bidding works.

He has been consulted by the EU Commission and the US Senate on the dangers for website visitors of processing personal data in the course of auctioning online advertising space [see https://www.iccl.ie/staff/dr-johnny-ryan/]. His research and commentary appear in media such as *The New York Times*, *The Economist*, *Wired*, *Le Monde* and on the front page of the *Financial Times*.

2. Defendant 1

The 1st defendant is an international association of media and technology companies engaged in digital advertising. The 1st defendant's members include technology companies such as Google, Facebook, and AT&T, among others.

Offer of Proof: Partial printout of the 1st defendant's website as of 03/23/2021 regarding IAB Tech Lab Members, available at: https://iabtechlab.com/about-the-iab-tech-lab/iab-tech-labq-members/, last accessed 03/23/2021,

presented as **Annex K 4**

The 1st defendant develops and promotes technologies and technical standards for fully

automated personalized online advertising, including the basic technical standard OpenRTB, which is substantiated by the further technical standards AdCOM, Content Taxonomy, and Audience Taxonomy. These standards form the framework for the global functioning of the targeting of personalized advertising media in the real-time auction of online advertising space on websites and in apps. In addition to developing these standards and protocols, the defendant also supports companies in their implementation.

The 1st defendant is operationally active in Europe through a German company, namely vonwersch Digital Strategies GmbH. Its managing director, Oliver von Wersch, and his employees oversee key areas of the defendant's activities in Europe:

> *"[...] The Founder and CEO of vonwerschpartner, Oliver von Wersch, will oversee key aspects of Tech Lab operations in the EU and UK. The overall vonwerschpartner organization will support Tech Lab with a cross-functional team of project managers and ad tech specialists to effectively serve the needs of the region."*
>
> *"Working with vonwerschpartner will help us build stronger, lasting relationships throughout Europe. As a global organization, it is crucial that we connect regularly with a broad range of members to understand their needs, share new developments, and facilitate standards adoption. [...]"*

Offer of Proof: Partial printout of 1st defendant's website, press release dated 09/06/2020, available at: https://iabtechlab.com/press-releases/tech-lab-increases-investment-presence-in-europe/, last accessed 12/02/2021,

presented as **Annex K 5**

Three employees of vonwersch Digital Strategies GmbH are assigned to the business premises in Hamburg to represent and implement the interests of the 1st defendant in Germany. They manage the main components of the operative business of the 1st defendant in Europe. These are sales and communication activities of the 1st defendant vis-à-vis members and departments of the IAB, Inc. in Europe as well as vis-à-vis the public, the involvement of European companies in the development of the standards and the organization of exchange meetings of the members concerning the implementations of the 1st defendant's technical standards.

> *"[...] What we do*
>
> *vonwerschpartner Digital Strategies represent IAB Tech Lab in Europe, with a dedicated staff of 3 people. We support the client in building up and extending long-term market relationships, e.g. with local IABs, develop*

strategic cooperations, represent the client on local events through panels and speeches, and support the engagement of (new) members.

Since the beginning of our mandate, we have significantly increased the awareness for Tech Lab's activities in Europe, and improved the active involvement of European companies, and other entities into the technology development processes (e.g. Project Rearc). […]"

Offer of Proof: Partial printout of vonwersch Digital Strategies GmbH website as of 02/12/2021 regarding Tech Lab Leadership, available at: https://vonwerschpartner.com/case-studies/iab-tech-lab, last accessed 02/12/2021, p. 4,

presented as **Annex K 6**

The 1st defendant's website states that this has significantly increased awareness of the work of the IAB TechLab in Europe and that this has improved the active involvement of European companies and other institutions in the technology development processes. The 1st defendant has publicly acknowledged that the engagement with vonwersch Digital Strategies GmbH is to facilitate the adoption of standards, and that this is done on the instructions of the 1st defendant ("on behalf of IAB Tech Lab").

Offer of Proof: Partial printout of 1st defendant's website, European Communication Groups, as of 03/23/2021, available at: https://iabtechlab.com/eea/, last accessed 03/23/2021,

presented as **Annex K 7**

3. Defendant 2

The 2nd defendant operates a technology platform which enables the purchase and sale of "inventory", i.e. advertising space on websites from several advertising networks (hereinafter "advertising exchange" or "online advertising exchange").

The 2nd defendant is a member of the 1st defendant (see partial printout of the 1st defendant's website dated 23/03/2021 via IAB Tech Lab Members, available at: https://iabtechlab.com/about-

the-iab-tech-lab/iab-tech-lab-members/, last accessed 23/03/2021, already submitted as **Annex K 4**).

Advertising Exchanges (online advertising exchanges) give access to an additional marketing channel for publisher websites (websites with advertising space), marketers (agencies) and ad networks, thus enabling advertisers to access advertising space from multiple website providers. In doing so, the second defendant in turn uses technology platforms that enable the automated and auction-based purchase of online advertising and its automated control in real time [see "Glossary" of the Bundesverband Digitale Wirtschaft (BVDW) e.V. of 23.03.2021, available at: https://www.bvdw.org/glossar/, last accessed on 23.03.2021].

The 2nd defendant is identified as a controller for the processing of personal data in the data protection notices for the platform of the online advertising exchange Xandr.

Offer of proof: Partial printout of the website of Xandr, Inc., Platform Privacy Policy, as amended 2/24/2021, available at: https://www.xandr.com/privacy/platform-privacy-policy/ , last accessed 4/14/2021,

presented as **Annex K 8**

2nd defendant maintains subsidiaries worldwide. These include, among others, the wholly owned subsidiary AppNexus, Inc. (28 West 23rd Street New York, NY 10010 USA). AppNexus, Inc. holds 100% of the shares in AppNexus Germany GmbH, a subsidiary based in Hamburg. According to the corporate purpose of AppNexus Germany GmbH, which is shown in the commercial register, the German branch is responsible for "The sale of, account management for, marketing of and implementation of real-time advertising technologies, in particular those of the shareholder AppNexus Inc. as well as the corresponding customer support and other related services".

Offer of proof: Printout of the extract from the commercial register of defendant 2 dated 23.03.2021,

presented as **Annex K 9**

The 2nd defendant is responsible for the implementation of the technical standards OpenRTB,

AdCOM, Content Taxonomy, and Audience Taxonomy, of the 1st defendant in Germany.

Defendant 2 is a subsidiary of WarnerMedia, a branch of the US telecommunications provider AT&T with an annual turnover of USD 171 billion in 2020 [see Key figures of AT&T, available at: https://www.finanzen.net/bilanz_guv/at_t, last accessed on 06.04.2021].

4. Defendant 3

The 3rd defendant operates an information service on the topics of online marketing and e-commerce under the website with the URL https://onlinemarketing.de. Reports on current developments in the industry appear there. Reports on current developments in the industry appear there. It also sells marketing services via this website, inter alia in the form of advertising space, paid contributions or e-mail advertising.

On Sept. 05, 2019, an article was published on defendant's website titled "Privacy Scandal: Secret Google Websites to Sell User Data?" reporting on plaintiff's activities.

Offer of Proof: Partial Printout of 3rd defendant's website, *Gau,* Secret Google Websites to Sell User Data? , Sept. 05, 2019, available at: https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten, last accessed Apr. 14, 2021,

presented as **Annex K 10**

II. Concerning motion 1

In the following, the general processes of Real Time Bidding (1.) as well as the function of the individual challenged standards are explained (2.). This is followed by a description of the processing of the plaintiff's personal data that is the subject of the dispute (3.). Then the deficits of the data security of the processing are described (4.). Finally, the responsibility contributions of the individual defendants follow (5.).

1. General functioning of Real Time Bidding

Real Time Bidding takes place behind the scenes of commercial websites and apps. When a data subject accesses a website such as that of the 3rd defendant, which participates in Real Time Bidding auctions according to the 1st defendant's specifications, each advertising space on a website is allocated by an automated auction in real time, on the basis of the data subject's precisely fitting personal data.

Defendant 1's system works as follows: Supply Side Platforms (SSPs) use defendant 1's technical standards to send out requests for bids on advertising space on the website. This bid request contains a variety of personal information about the person who loads the website or app.

SSPs and online advertising exchanges that enable the buying and selling of advertising space from multiple advertising networks (Advertising Exchanges), such as the 2nd defendant, send this personal data to a large number of other companies called Demand Side Platforms (DSPs) that act on behalf of advertisers.

There may also be auctions of auctions, in which several online advertising exchanges (Advertising Exchanges), such as that of the 2nd defendant, each send bid requests to a large number of companies to solicit bids for a single advertising space (so-called header bidding).

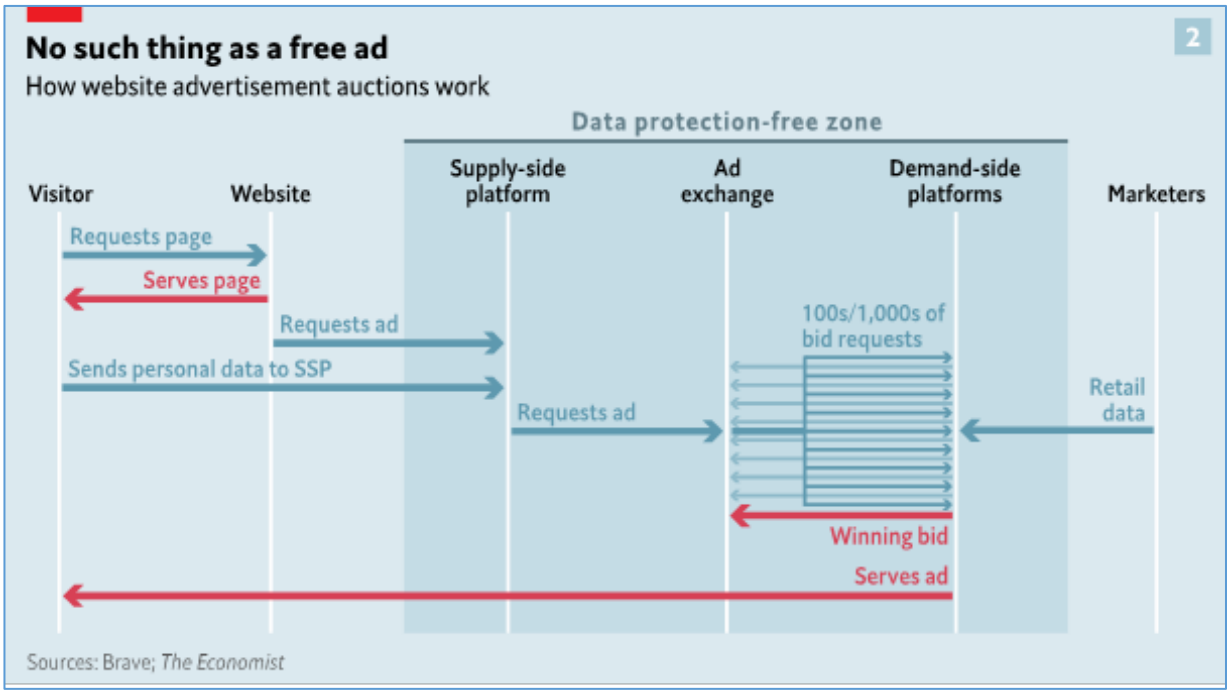
Offer of Proof: Entire printout of defendant 1's website, Standard Header Container Integration with an Ad Server, as amended June 2017, available at: https://iabtechlab.com/wp-content/uploads/2016/07/IABTechLabStandardHeaderContainerIntegrationwithanAdServer_DRAFTforpubliccomment.pdf, last accessed 03/23/2021,

presented as **Annex K 11**

When a SSP sends a bid request about a particular individual to a DSP, possibly through an online advertising exchange, DSPs then decide whether, and how much, to bid for the opportunity to display an advertisement to that individual, based on the information they received in the bid request.

In less than a second (less than 200 milliseconds), the ad that won the auction is loaded on the website. This process can take place several times while a website is loading, to auction each of the advertising spaces available on the specific website.

The following diagram, prepared by the international weekly newspaper *The Economist in* collaboration with plaintiff, shows the flow of information from an IAB OpenRTB auction that takes place to auction off a single advertising slot [*The Economist*, Mar. 23, 2019, p. 21.].



In its specifications, the 1st defendant itself speaks of the fact that a single auction based on its OpenRTB technical standard results in thousands of companies receiving the personal data in a single bid request, and that publishers fear liability risks arising from this:

> *"Surfacing thousands of vendors with broad rights to use data w/out tailoring those rights may be too many vendors/permissions [...]".*

The 1st defendant also acknowledged that there is no technical control over the data after it has been sent out in an auction.

Offer of Proof: Entire printout of the technical specification of defendant 1 and IAB Europe A.I.S.B.L. , Pubvendors.json v1.0: Transparency & Consent Framework, as amended May 2018, available at:

https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md, last accessed 23/03/2021,

submitted as **Annex K 12**

According to the 2nd defendant, 1647 companies can receive a bid request from it.

Offer of Proof: Partial printout of the website of Xandr, Inc., Third Party Providers, as of 12/01/2021, available at https://docs.xandr.com/bundle/service-policies/page/third-party-providers.html#ThirdPartyProviders-Ad-serverPartners, last accessed 03/24/2021,

presented as **Annex K 13**

Art. 4 No. 1 GDPR defines the term personal data:

> *"[...] '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; [...]."*

Recital 30 of the GDPR clarifies that online identifiers can be attributed to natural persons.

> *"[...] 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.. [...]"*

In bid requests based on the technical standard OpenRTB of the 1st defendant the following data may be included:

- the location, including postcode and GPS data;

- the person's place of residence (which does not have to be the same as the current location);
- the web content that the person is viewing, reading or listening to on their device ("site", "app");
- Identifiers of the person, including
    - the Advertising Exchange identifier ("ID");
    - the Demand Side Platform (DSP) identifier ("buyeruid");
    - a personal identifier of the individual used by a DSP and an advertising exchange in a consistent manner ("Extended Identifier UIDs");
    - an identifier of the individual that includes information about which apps they use and which websites they visit ("consent string");
    - unique device identifiers, such as the IMEI and MAC address, encrypted in a way in which they remain unique identification codes (in early versions OpenRTB Specifications v2.4 and v2.5);
    - the mobile advertising identifier ("ifa");
    - the year of birth of the person, if known;
    - the sex of the person, if known;
    - "Ext[ension]", fields that allow the advertising exchange to add additional data, including special categories, about the individual;
    - the individual's interests, based on which websites they visit or which apps they use (this may include very sensitive personal characteristics such as religion, political views, sexuality and health, for more details see A. IV. 2. b) bb), p. 105;
    - the "segments" into which the person has been classified (the classification is based on profile data that originate either from the Advertising Exchange itself or from third parties, and may include highly sensitive information about religion, political views, sexuality or health - for example, the list of the 1st defendant contains the segment "Cancer", for more details see A. IV. 2. b) cc), p. 110;
    - the device characteristics, including:
        - IP address;
        - Height, width and aspect ratio of the screen;
        - Device manufacturer, model, version;
        - JavaScript support, if applicable;
        - Operating system including version;

- Browser software and version;
- Flash version supported by the browser;
- Language;
- Telecommunication provider, type of connection, in case of mobile connection type of network.

Defendant 1's current OpenRTB Specifications v3.0 protocol references defendant 1's AdCOM Specifications v1.0 to specify the data contained in the Bid Request:)

Object: Request

The `Request` object contains a globally unique bid request ID. This `id` attribute is required as is an `Item` array with at least one object (i.e., at least one item for sale). Other attributes establish rules and restrictions that apply to all items being offered. This object also interfaces to Layer-4 domain objects for context such as the user, device, site or app, etc.

Attribute	Type	Definition
`id`	string; required	Unique ID of the bid request; provided by the exchange.
`test`	integer; default 0	Indicator of test mode in which auctions are not billable, where 0 = live mode, 1 = test mode.
`tmax`	integer	Maximum time in milliseconds the exchange allows for bids to be received including Internet latency to avoid timeout. This value supersedes any general guidance from the exchange. If an exchange acts as an intermediary, it should decrease the outbound `tmax` value from what it received to account for its latency and the additional internet hop.
`at`	integer; default 2	Auction type, where 1 = First Price, 2 = Second Price Plus. Values greater than 500 can be used for exchange-specific auction types.
`cur`	string array; default ["USD"]	Array of accepted currencies for bids on this bid request using ISO-4217 alpha codes. Recommended if the exchange accepts multiple currencies. If omitted, the single currency of "USD" is assumed.
`seat`	string array	Restriction list of buyer seats for bidding on this item. Knowledge of buyer's customers and their seat IDs must be coordinated between parties beforehand. Omission implies no restrictions.
`wseat`	integer; default 1	Flag that determines the restriction interpretation of the `seat` array, where 0 = block list, 1 = whitelist.
`cdata`	string	Allows bidder to retrieve data set on its behalf in the exchange's cookie (refer to `cdata` in Object: Response) if supported by the exchange. The string must be in base85 cookie-safe characters.
`source`	object	A `Source` object that provides data about the inventory source and which entity makes the final decision. Refer to Object: Source.
`item`	object array; required	Array of `Item` objects (at least one) that constitute the set of goods being offered for sale. Refer to Object: Item.
`package`	integer	Flag to indicate if the Exchange can verify that the items offered represent all of the items available in context (e.g., all impressions on a web page, all video spots such as pre/mid/post roll) to support road-blocking, where 0 = no, 1 = yes.
`context`	object; recommended	Layer-4 domain object structure that provides context for the items being offered conforming to the specification and version referenced in `openrtb.domainspec` and `openrtb.domainver`. For AdCOM v1.x, the objects allowed here all of which are optional are one of the `DistributionChannel` subtypes (i.e., `Site`, `App`, or `Dooh`), `User`, `Device`, `Regs`, `Restrictions`, and any objects subordinate to these as specified by AdCOM.
`ext`	object	Optional exchange-specific extensions.

Offer of Proof: Partial printout of 1st defendant's Technical Specifications, OpenRTB Specifications v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#object_request, last accessed Feb. 11,

2021,

submitted as **Annex K 14**

Bid Request

The following is an example of Layer-3 of a bid request with a single item offered for sale and a single private marketplace deal associated with it. Some optional attributes have been omitted for brevity. Notice that `spec` and `context` are the interfaces to domain objects specified in AdCOM. The `spec` object should have one `placement` object that carries the details of the impression being offered under this item. The `context` object can have any of `device`, `user`, `regs`, `restrictions`, and at most one of `site` (shown in the example), `app`, or `dooh`.

```
{
   "openrtb": {
      "ver": "3.0",
      "domainspec": "adcom",
      "domainver": "1.0",
      "request": {
         "id": "0123456789ABCDEF",
         "tmax": 150,
         "at": 2,
         "cur": [ "USD", "EUR" ],
         "source": {
            "tid": "FEDCBA9876543210",
            "ts": 1541796182157,
            "ds": "AE23865DF890100BECCD76579DD4769DBBA9812CEE8ED90BF",
            "dsmap": "...",
            "cert": "ads-cert.1.txt",
            "pchain": "..."
         },
         "package": 0,
         "item": [
            {
               "id": "1",
               "qty": 1,
               "private": 0,
               "deal": [
                  {
                     "id": "1234",
                     "flr": 1.50
                  }
               ],
               "spec": {
                  "placement": {  Refer to the AdCOM Specification.  }
               }
            }
         ],
         "context": {
            "site": {  Refer to the AdCOM Specification.  },
            "user": {  Refer to the AdCOM Specification.  },
            "device": {  Refer to the AdCOM Specification.  },
            "regs": {  Refer to the AdCOM Specification.  },
            "restrictions": {  Refer to the AdCOM Specification.  }
         }
      }
   }
}
```

Offer of Proof: Partial Printout: Example Bid Request under 1st defendant's Technical Specifications, OpenRTB Specification v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#bidrequest, last accessed Feb. 11, 2021,

presented as **Annex K 15**

Offer of Proof: Entire printout of 1st defendant's Technical Specifications, OpenRTB Specification v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#,%20zuletzt%20abgerufen%20am%2026.03.2021,

presented as **Annex K 16**

The technical specification AdCOM Specifications v1.0 of the 1st defendant defines the individual personal data contained in a bid request, e.g. the location (Object: Geo), the environment of the visited website (Object: Site) or the app used (Object: App), the website operator (Object: Publisher), the user's personal information already collected from other website visits or other sources (Object: User, Data and Segment) and the user's terminal device (Object: Device) (smartphone, tablet, desktop PC, laptop, smart TV device, etc.).

Object: Geo

This object encapsulates various methods for specifying a geographic location. When subordinate to a `Device` object, it indicates the location of the device which can also be interpreted as the user's current location. When subordinate to a `User` object, it indicates the location of the user's home base (i.e., not necessarily their current location).

The `lat` and `lon` attributes should only be passed if they conform to the accuracy depicted in the `type` attribute. For example, the centroid of a large region (e.g., postal code) should not be passed.

Attribute	Type	Definition
`type`	integer	Source of location data; recommended when passing lat/lon. Refer to List: Location Types.
`lat`	float	Latitude from -90.0 to +90.0, where negative is south.
`lon`	float	Longitude from -180.0 to +180.0, where negative is west.
`accur`	integer	Estimated location accuracy in meters; recommended when lat/lon are specified and derived from a device's location services (i.e., type = 1). Note that this is the accuracy as reported from the device. Consult OS specific documentation (e.g., Android, iOS) for exact interpretation.
`lastfix`	integer	Number of seconds since this geolocation fix was established. Note that devices may cache location data across multiple fetches. Ideally, this value should be from the time the actual fix was taken.
`ipserv`	integer	Service or provider used to determine geolocation from IP address if applicable (i.e., `type` = 2). Refer to List: IP Location Services.
`country`	string	Country code using ISO-3166-1-alpha-2. *Note that alpha-3 codes may be encountered and vendors are encouraged to be tolerant of them.*
`region`	string	Region code using ISO-3166-2; 2-letter state code if USA.
`metro`	string	Regional marketing areas such as Nielsen's DMA codes or other similar taxonomy to be agreed among vendors prior to use. *Note that DMA is a trademarked asset of The Nielsen Company. Vendors are encouraged to ensure their use of DMAs is properly licensed.*
`city`	string	City using United Nations Code for Trade & Transport Locations "UN/LOCODE" with the space between country and city suppressed (e.g., Boston MA, USA = "USBOS"). Refer to UN/LOCODE Code List.
`zip`	string	ZIP or postal code.
`utcoffset`	integer	Local time as the number +/- of minutes from UTC.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_geo, last accessed 03/24/2021,

presented as **Annex K 17**

Object: Site

Derived from: DistributionChannel

This object is used to define an ad supported website, in contrast to a non-browser application, for example. As a derived class, a `site` object inherits all `DistributionChannel` attributes and adds those defined below.

Attribute	Type	Definition
`domain`	string	Domain of the site (e.g., "mysite.foo.com").
`cat`	string array	Array of content categories describing the site using IDs from the taxonomy indicated in `cattax`.
`sectcat`	string array	Array of content categories describing the current section of the site using IDs from the taxonomy indicated in `cattax`.
`pagecat`	string array	Array of content categories describing the current page or view of the site using IDs from the taxonomy indicated in `cattax`.
`cattax`	integer	The taxonomy in use for the `cat`, `sectcat` and `pagecat` attributes. Refer to List: Category Taxonomies.
`privpolicy`	integer	Indicates if the site has a privacy policy, where 0 = no, 1 = yes.
`keywords`	string	Comma separated list of keywords about the site.
`page`	string	URL of the page within the site.
`ref`	string	Referrer URL that caused navigation to the current page.
`search`	string	Search string that caused navigation to the current page.
`mobile`	integer	Indicates if the site has been programmed to optimize layout when viewed on mobile devices, where 0 = no, 1 = yes.
`amp`	integer	Indicates if the page is built with AMP HTML, where 0 = no, 1 = yes.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's Protocol Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_site, last accessed 03/24/2021,

submitted as **Annex K 18**

Object: Publisher

This object describes the publisher of the media in which ads will be displayed.

Attribute	Type	Definition
`id`	string, recommended	Vendor-specific unique publisher identifier, as used in ads.txt files.
`name`	string	Displayable name of the publisher.
`domain`	string	Highest level domain of the publisher (e.g., "publisher.com").
`cat`	string array	Array of content categories that describe the publisher using IDs from the taxonomy indicated in `cattax`. Implementer should ensure compliance with regional legislation around data usage and sharing.
`cattax`	integer	The taxonomy in use for the `cat` attribute. Refer to List: Category Taxonomies.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's technical specifications, AdCOM

Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_publisher, last accessed 03/22/2021,

submitted as **Annex K 19**

Object: User

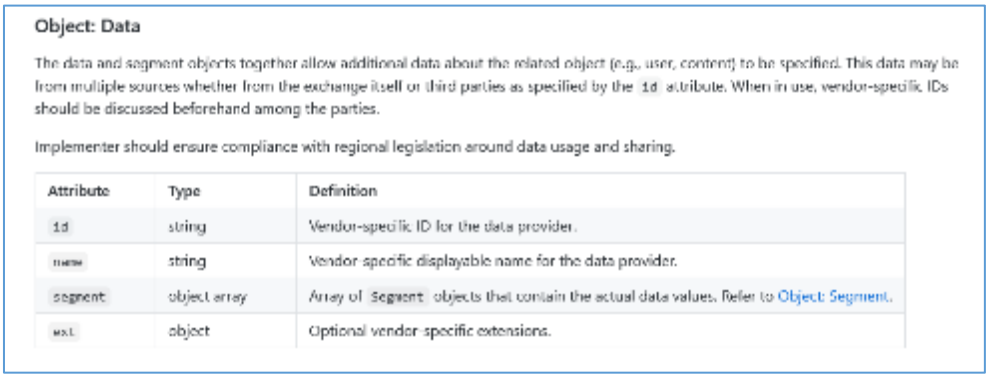
This object contains information known or derived about the human user of the device (i.e., the audience for advertising). The user ID is a vendor-specific artifact and may be subject to rotation or other privacy policies. However, this user ID must be stable long enough to serve reasonably as the basis for frequency capping and retargeting.

Implementer should ensure compliance with regional legislation around data usage and sharing.

Attribute	Type	Definition
`id`	string; recommended	Vendor-specific ID for the user. At least one of `id` or `buyeruid` is strongly recommended.
`buyeruid`	string; recommended	Buyer-specific ID for the user as mapped by an exchange for the buyer. At least one of `id` or `buyeruid` is strongly recommended.
`yob`	integer	Year of birth as a 4-digit integer.
`gender`	string	Gender, where "M" = male, "F" = female, "O" = known to be other (i.e., omitted is unknown).
`keywords`	string	Comma separated list of keywords, interests, or intent.
`consent`	string	GDPR consent string if applicable, complying with the comply with the IAB standard Consent String Format in the Transparency and Consent Framework technical specifications.
`geo`	object	Location of the user's home base (i.e., not necessarily their current location). Refer to Object: Geo.
`data`	object array	Additional user data. Each `Data` object represents a different data source. Refer to Object: Data.
`eids`	object	Extended (third-party) identifiers for this user. Refer to Object: Extended Identifiers.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_user, last accessed 03/24/2021,

presented as **Annex K 20**



Object: Data

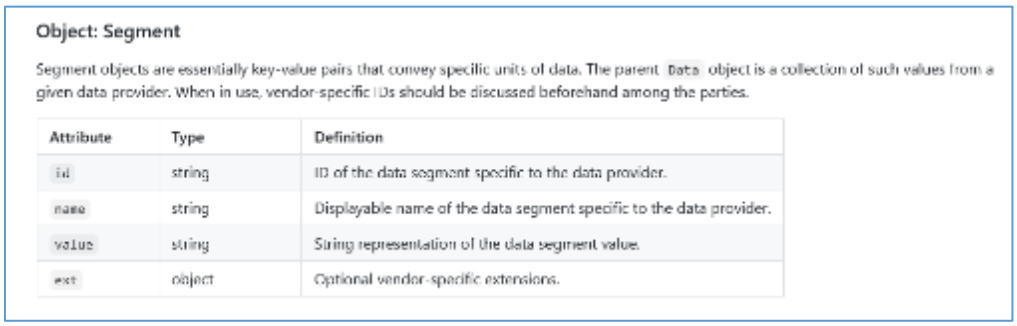
The data and segment objects together allow additional data about the related object (e.g., user, content) to be specified. This data may be from multiple sources whether from the exchange itself or third parties as specified by the `id` attribute. When in use, vendor-specific IDs should be discussed beforehand among the parties.

Implementer should ensure compliance with regional legislation around data usage and sharing.

Attribute	Type	Definition
`id`	string	Vendor-specific ID for the data provider.
`name`	string	Vendor specific displayable name for the data provider.
`segment`	object array	Array of `Segment` objects that contain the actual data values. Refer to Object: Segment.
`ext`	object	Optional vendor specific extensions.

Offer of Proof: Partial printout of 1st defendant's technical specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_data, last accessed 03/22/2021,

presented as **Annex K 21**



Object: Segment

Segment objects are essentially key-value pairs that convey specific units of data. The parent `Data` object is a collection of such values from a given data provider. When in use, vendor-specific IDs should be discussed beforehand among the parties.

Attribute	Type	Definition
`id`	string	ID of the data segment specific to the data provider.
`name`	string	Displayable name of the data segment specific to the data provider.
`value`	string	String representation of the data segment value.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's technical specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_segment, last accessed 03/22/2021,

submitted as **Annex K 22**

Object: Device

This object provides information pertaining to the device through which the user is interacting. Device information includes its hardware, platform, location, and carrier data. The device can refer to a mobile handset, a desktop computer, set top box, or other digital device.

Implementer should ensure compliance with regional legislation around data usage and sharing.

Attribute	Type	Definition
`type`	integer	The general type of device. Refer to List: Device Types.
`ua`	string	Browser user agent string.
`ifa`	string	ID sanctioned for advertiser use in the clear (i.e., not hashed).
`dnt`	integer	Standard "Do Not Track" flag as set in the header by the browser, where 0 = tracking is unrestricted, 1 = do not track.
`lmt`	integer	"Limit Ad Tracking" signal commercially endorsed (e.g., iOS, Android), where 0 = tracking is unrestricted, 1 = tracking must be limited per commercial guidelines.
`make`	string	Device make (e.g., "Apple").
`model`	string	Device model (e.g., "iPhone10,1" when the specific device model is known, "iPhone" otherwise). The value obtained from the device O/S should be used when available.
`os`	integer	Device operating system. Refer to List: Operating Systems.
`osv`	string	Device operating system version (e.g., "3.1.2").
`hwv`	string	Hardware version of the device (e.g., "5S" for iPhone 5S).
`h`	integer	Physical height of the screen in pixels.
`w`	integer	Physical width of the screen in pixels.
`ppi`	integer	Screen size as pixels per linear inch.
`pxratio`	float	The ratio of physical pixels to device independent pixels.
`js`	integer	Support for JavaScript, where 0 = no, 1 = yes.
`lang`	string	Browser language using ISO-639-1-alpha-2.
`ip`	string	IPv4 address closest to device.
`ipv6`	string	IP address closest to device as IPv6.
`xff`	string	The value of the "x-forwarded-for" header.
`iptr`	integer	Indicator of truncation of any of the IP attributes (i.e., `ip`, `ipv6`, `xff`), where 0 = no, 1 = yes (e.g., from 1.2.3.4 to 1.2.3.0). Refer to https://tools.ietf.org/html/rfc6235#section-4.1.1 for more information on IP truncation.
`carrier`	string	Carrier or ISP (e.g., "VERIZON") using exchange curated string names which should be published to bidders beforehand.
`mccmnc`	string	Mobile carrier as the concatenated MCC-MNC code (e.g., "310-005" identifies Verizon Wireless CDMA in the USA). Refer to https://en.wikipedia.org/wiki/Mobile_country_code for further information and references. Note that the dash between the MCC and MNC parts is required to remove parsing ambiguity.
`mccmncsim`	string	MCC and MNC of the SIM card using the same format as `mccmnc`. When both values are available, a difference between them reveals that a user is roaming.
`contype`	integer	Network connection type. Refer to List: Connection Types.
`geofetch`	integer	Indicates if the geolocation API will be available to JavaScript code running in display ad, where 0 = no, 1 = yes.
`geo`	object	Location of the device (i.e., typically the user's current location). Refer to Object: Geo.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's Technical Specifications, AdCOM

Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_device, last accessed 03/24/2021,

submitted as **Annex K 23**

Offer of Proof: Entire printout of 1st defendant's Protocol Technical Specifications, AdCOM Specifications v1.0, June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md, last accessed 03/24/2021,

submitted as **Annex K 24**

The personal data contained in a bid request allows anyone who receives it to build a long-term dossier of intimate behaviors and characteristics of the site visitor, including movement profile, political views, religion, sexuality, and health status.

2. Role of the respective standards

a) OpenRTB

The OpenRTB technical specification of the 1st defendant forms the basis for communication between publisher websites offering advertising space, and advertisers, SSPs and DSPs, online advertising exchanges, and other intermediaries in the trade of online advertising space for automatically served advertising media. It defines the process of auctions of advertising spaces and ensures the interoperability of the communication processes between the entities involved by defining the formats and structure of bid requests and bid responses, as well as parameters for the auctions.

It sets the rules for what data can and should be included in the bid requests that SSPs and advertising exchanges send to DSPs, and how those requests are transmitted.

Several versions of the specification are currently in use, including v2.4, v2.5, and v3.0.

b) AdCOM

The technical standard of the 1st defendant AdCOM (Advertising Common Object Model) is a supplement to the specification of the defendant OpenRTB. AdCOM describes, among other things, the exact contents of the "objects" exchanged within the framework of OpenRTB, i.e. the types of personal data in bid requests as well as the structure of the bid requests, the bids and the transmitted advertising media. AdCOM enables the standardized dissemination of personal data in bid requests.

The AdCOM specification was integrated into the OpenRTB specification in early versions of the specification.

c) Content Taxonomy

The technical standard of the 1st defendant Content Taxonomy is a table that standardizes over 1000 categories for web content, assigns them an ID and assigns them to supercategories. This creates the possibility to record information about the context of the queried web content in a standardized way and to exchange it automatically. Content Taxonomy is a technical prerequisite for the automated enrichment of user profiles with information about user interests and facilitates data exchange considerably.

The Content Taxonomy specification was integrated into the OpenRTB specification in early versions of the specification.

According to the 1st defendant, the Content Taxonomy standard is intended to create a "lingua franca" that all parties - SSPs, DSPs and advertisers - can use and understand when describing the content of a website or app. Content Taxonomy is also used for contextual advertising and to ensure that ads for brands are presented in an appropriate environment.

Offer of Proof: Entire printout of 1st defendant's website, Implementation Guide for Brand Suitability with the Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/wp-content/uploads/2020/12/Implementation_Guide_for_Brand_Suitability_with_IABTechLab_Content_Taxonomy_2-2.pdf), last accessed 03/23/2021, p. 4,

presented as **Annex K 25**

There are currently several versions of Content Taxonomy in use. The current version is v2.2. For more details, see A. IV. 2. b), p. 107.

d) Audience Taxonomy

Similar to Content Taxonomy, the defendant's technical specification Audience Taxonomy standardizes properties in an Excel file. Unlike Content Taxonomy, however, it deals with properties of users instead of content. Audience Taxonomy contains more than 1500 segments, a variety of demographic factors such as gender, educational background, income, buyer interests, other interests, and hobbies. Each category is assigned an ID. The taxonomy allows the standardized exchange of personal data about the user concerned in the context of an auction. OpenRTB bid requests may contain segments to which a user has been assigned.

There are currently several versions of Audience Taxonomy in use. The current version is version 1.1.

More details are given under point A. IV. 2. c), p. 117.

3. Processing of personal data of the plaintiff, triggered by visiting the website of defendant 3

On 25.03.2021, the plaintiff accessed the website of the 3rd defendant under the URL https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten. The URL contains an article describing possible data protection violations by Google and mentions the plaintiff's work.

On the website of the 3rd defendant there were several advertising spaces which were auctioned off in real time to the highest bidder via a DSP on the basis of the plaintiff's personal data when the website was called up.

This is evidenced by the simple use of the so-called developer console of a user's browser software, which measured network connections (HTTP transactions) of the 3rd defendant's website with

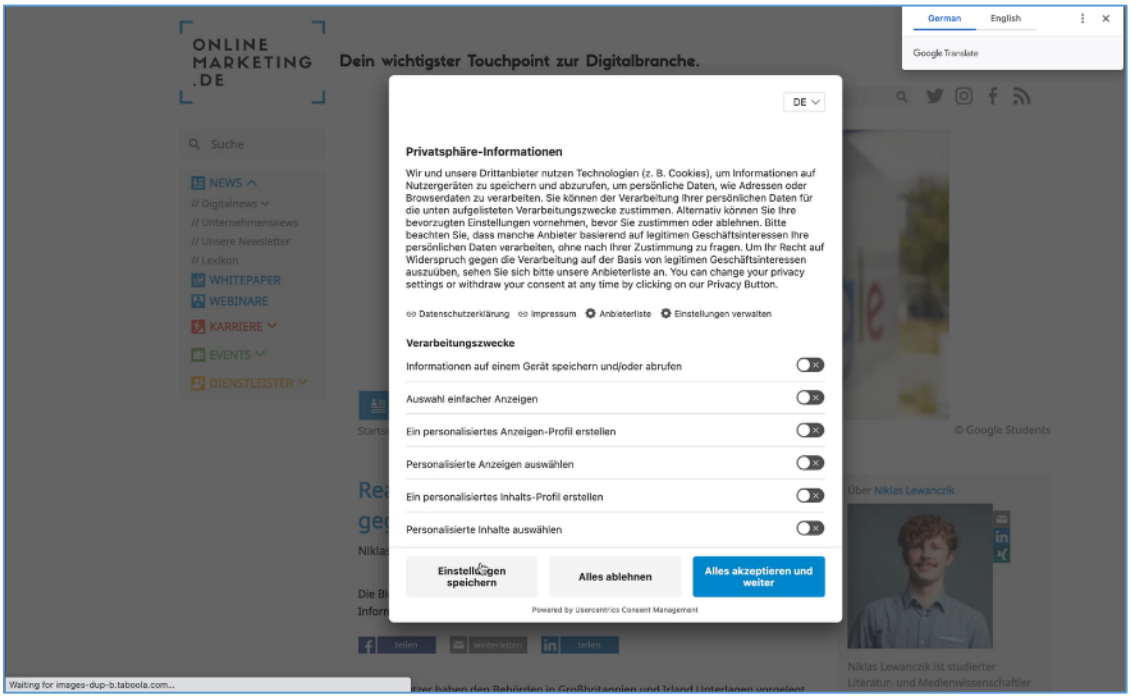
servers of the 2nd defendant in real time, as well as the implementation of a JavaScript of the 2nd defendant in the source code of the 3rd defendant's website. The technical standards of the 1st defendant were used.

In addition, the storage of information in the browser of the plaintiff's terminal device in cookies could be observed, as could the access to information in the browser of the plaintiff's terminal device by the 2nd defendant. Data transmissions triggered by this for the real-time auction of advertising spaces of the 3rd defendant could also be observed.

Anyone can open the developer console, for example, in the Firefox browser by pressing CTRL+SHIFT+K (in Microsoft EDGE by pressing F12, in Chrome by pressing CTRL+SHIFT+J) and, even without in-depth technical knowledge, can follow the processes described above in real time by observing the events displayed in the developer console.

In the following, it is shown on the basis of the real-time analysis of the network connections that personal data of the plaintiff were processed when the plaintiff loaded the website of the 3rd defendant, and when the plaintiff accepted the preset "privacy information" in the context of Real Time Bidding via the 2nd defendant as an online advertising exchange and the accompanying real-time auction. A real-time analysis of the data transmissions occurring when loading the website of the 3rd defendant under the URL https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten was carried out using the developer console on a standard Chrome browser (version 89.0.4389.90) with a standard MacBook (operating system: Mac OS X 11_2_1) from the plaintiff's location in Dublin.

Plaintiff accessed defendant 3's website at the URL https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten on 3/25/2021.



Offer of Proof: Printout of the home page of the website at the URL www.onlinemarketing.de of the 3rd defendant dated 25/03/2021,

submitted as **Annex K 26**

a) Real-time auction via "OpenRTB API Specification Version 2.4 "

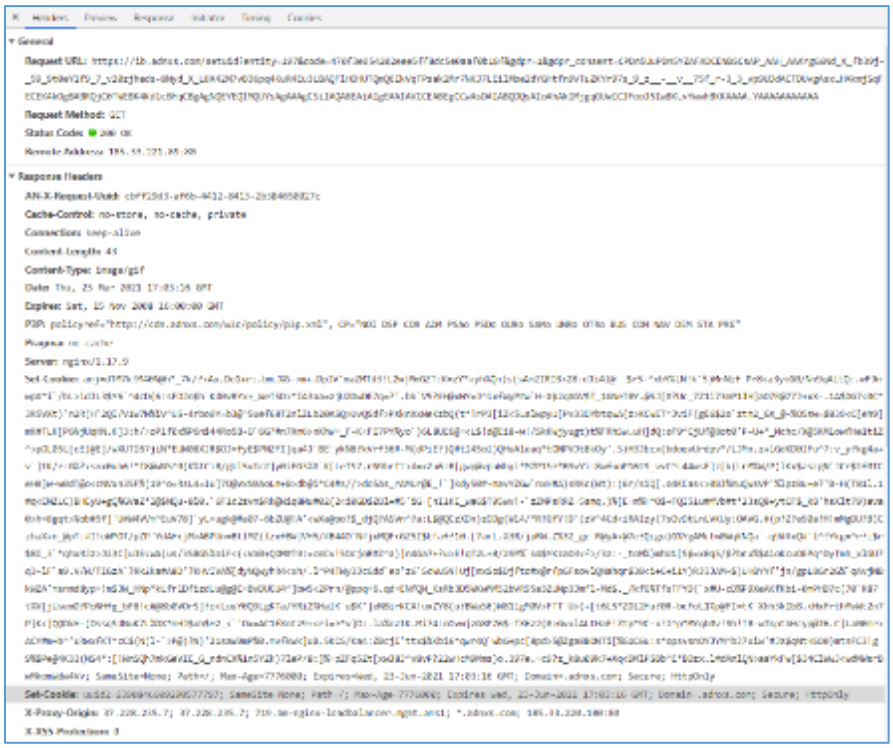
(1) JavaScripts and image pixels (tracking pixels) of the 2nd defendant that trigger the data processing in dispute are integrated in the source code of the 3rd defendant's website.

JavaScript is a “scripting” computer language, developed for dynamic HTML in web browsers to evaluate user interactions on websites, to change, reload or generate content. The 2nd defendant’s JavaScripts cause server requests to the 2nd defendant and the storage and accessing of cookies on the plaintiff's browser.

The tracking pixels are small, invisible image files that are loaded by the plaintiff's browser from the 2nd defendant's server and are enabled to do so by the 3rd defendant's website. These server requests to the 2nd defendant enable it to store and read cookies on the plaintiff's browser.

When the plaintiff called up the website at the URL

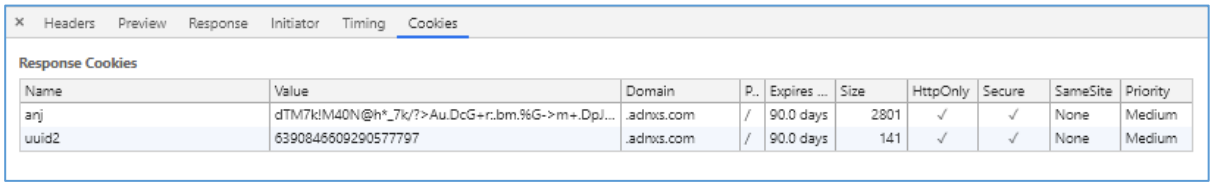
https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten on March 25, 2021 at 5:03 p.m. (GMT+0, corresponding to 6:03 p.m. German time), a server request was sent from the plaintiff's browser ("Request URL") to the 2nd defendant (https://ib.adnxs.com/setuid?entity=) with the request to set a cookie and assign a user ID in the browser of the plaintiff's terminal ("setuid") due to the corresponding programming of the 3rd defendant's website source code. The corresponding server response ("Response Headers") of the 2nd defendant assigned the plaintiff a User ID with the value (uuid2=6390846609290577797), which was stored in the plaintiff's browser in the 2nd defendant's cookie with the designation "uuid2".



Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with defendant 2,

submitted as **Annex K 27**

As a result of defendant 2's server response, the User ID (6390846609290577797) assigned by defendant 2 was stored in defendant 2's cookie (uuid2) in plaintiff's browser.



Headers Preview Response Initiator Timing Cookies

Response Cookies

Name	Value	Domain	P..	Expires ...	Size	HttpOnly	Secure	SameSite	Priority
anj	dTM7k!M40N@h*_7k/?>Au.DcG+r:.bm.%G->m+.DpJ...	.adnxs.com	/	90.0 days	2801	✓	✓	None	Medium
uuid2	6390846609290577797	.adnxs.com	/	90.0 days	141	✓	✓	None	Medium

Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with defendant 2 and browser web storage,

submitted as **Annex K 28**

(2) This User ID (6390846609290577797) of the plaintiff is matched with other User IDs of the plaintiff previously assigned by DSPs and SSPs, as well as data management platforms (DMP), in advance of the real-time auction of advertising spaces on the website of the 3rd defendant. Due to the matching process (cookie matching) of the User ID of the 2nd defendant with an indefinite number of User IDs of DSPs, SSPs, and DMPs, all parties involved in Real Time Bidding can clearly identify the plaintiff.

The server of the 2nd defendant transmits the user ID of the plaintiff as a parameter (e.g. www.partner.de?uui2=User123) to all connected DSPs, SSPs, and DMPs. The connected SSPDSPs, SSPs, and DMPs can read this user ID from the parameter as well as their own user ID in the cookie at www.partner.de. The user ID of the plaintiff can also be read out from the cookie. The SSPs, DSPs and DMPs can then synchronize their User IDs about the plaintiff and store them for future communication between the systems. URL information with parameters and categories of the URL are used to synchronize the User IDs.

On its website, the 2nd defendant states:

> *"When we get an ad call, we have to know the user's Xandr user ID so we can apply frequency and recency, segment, and other data. We can easily do this when our tag is on the page (i.e., the tag domain is ib.adnxs.com or has been CNAMEd to ib.adnxs.com) because we can access the user's ib.adnxs.com browser cookie where we store a Xandr ID."*

Offer of Proof: Partial printout of 2nd defendant's website, User ID Syncing with External Partners, as amended 03/31/2021, available at:

https://docs.xandr.com/bundle/invest_invest-standard/page/topics/user-id-syncing-with-external-partners.html, last accessed 03/31/2021,

presented as **Annex K 29**

When the plaintiff accessed the website https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten on 25.03.2021 at 17:04 (GMT+0, corresponding to 18:04 German time), it was observed during the real-time analysis of the outgoing network connections that code implemented in the source code of the website of the 3rd defendant triggered four requests to servers of the 2nd defendant with the designation (https://ib.adnxs.com/async_usersync?cbfn), which sent plaintiff's personal data to connected DSPs, SSPs, and DMPs, enabling the matching of User IDs for plaintiff.

Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with defendant 2,

submitted as **Annex K 30**

(3) The real-time analysis on 25.03.2021 revealed that the 3rd defendant uses “header bidding” for the real-time auction of advertising spaces (cf. in this regard already point A. II. 3. a), p. 30).

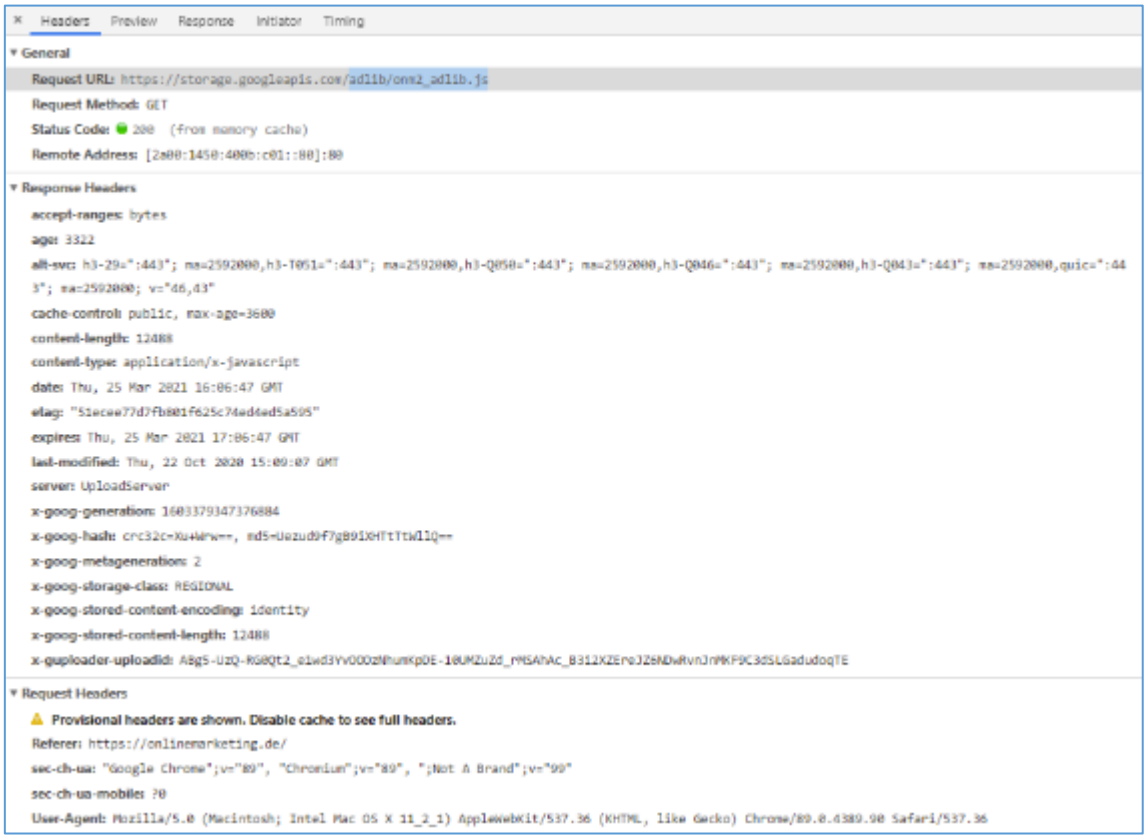
Based on Code implemented in the source code of the 3rd defendant, the 2nd defendant, among others, sent several bidding requests to an unspecified number of DSPs. It was established that the technical standard OpenRTB of the 1st defendant was used to conduct the auctions. In the process, several bid responses were sent back to the 2nd defendant by the DSPs, from which some details of the real-time auctions carried out can be gathered. In detail, the course of the auction is as follows:

(4) The 3rd defendant used “header bidding” to maximize the number of companies bidding on its advertising inventory. As a result, each ad space was routed to multiple SSPs. An auction of auctions took place for each advertising space, with the winning bid selected from the bids that won each auction. The result of the auction was communicated by the 2nd defendant in the server response of the respective DSP. Thus, there was a further duplication of the plaintiff's personal data when he loaded an online article that appeared about him.

The existence of header bidding on the 3rd defendant’s website was evident from a “call stack”: the sequence of server requests to individual SSPs as well as to the 2nd defendant's online advertising exchange. Among other things, the relevant server request for the execution of real time bidding was also made to the 2nd defendant.

The server requests triggered when visiting the 3rd defendant's website proceeded as follows:

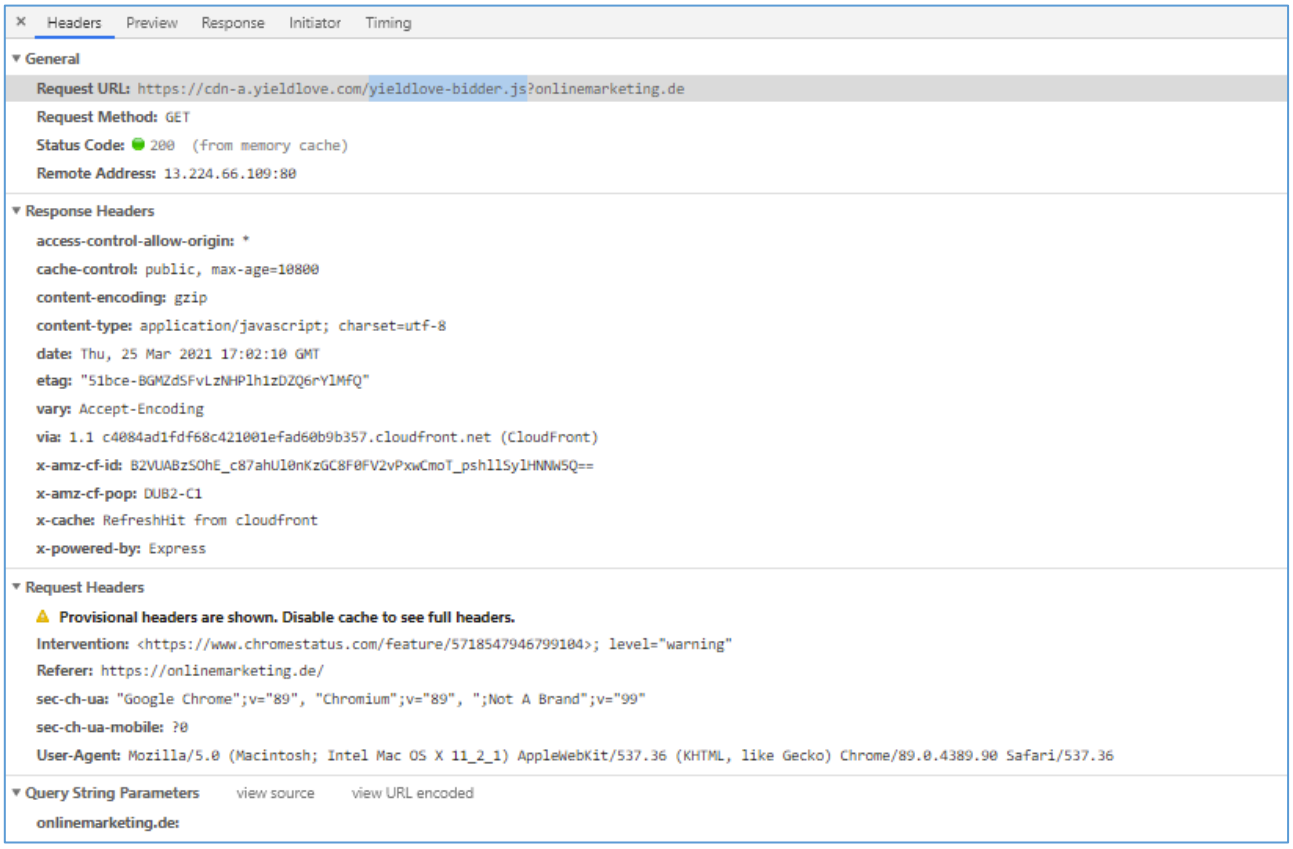
(a) Loading the JavaScript "adlib/onm2_adlib.js" from a Google server. This JavaScript configures available advertising space and third-party providers such as the defendant 2.



Offer of Proof: partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with defendant 2,)

submitted as **Annex K 31**

(b) Loading the header bidding JavaScript "yieldlove-bidder.js" (cf. following figure) from "Yieldlove" (Yieldlove GmbH, Kehrwieder 9, 20457 Hamburg), to coordinate the header bidding (i.e. which DSPs are used in which order based on which rules).

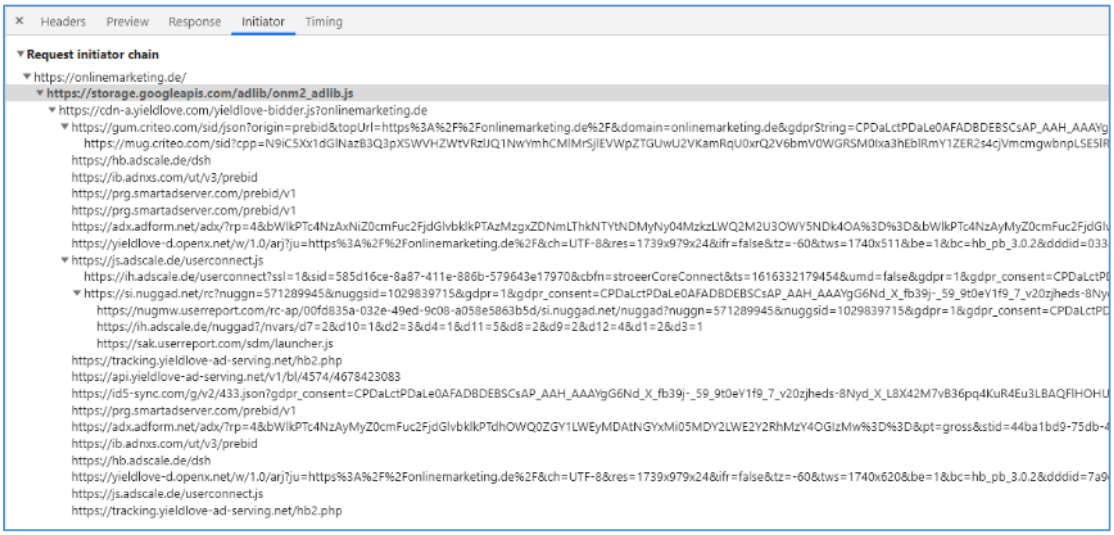


Offer of Proof: partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with defendant 2,)

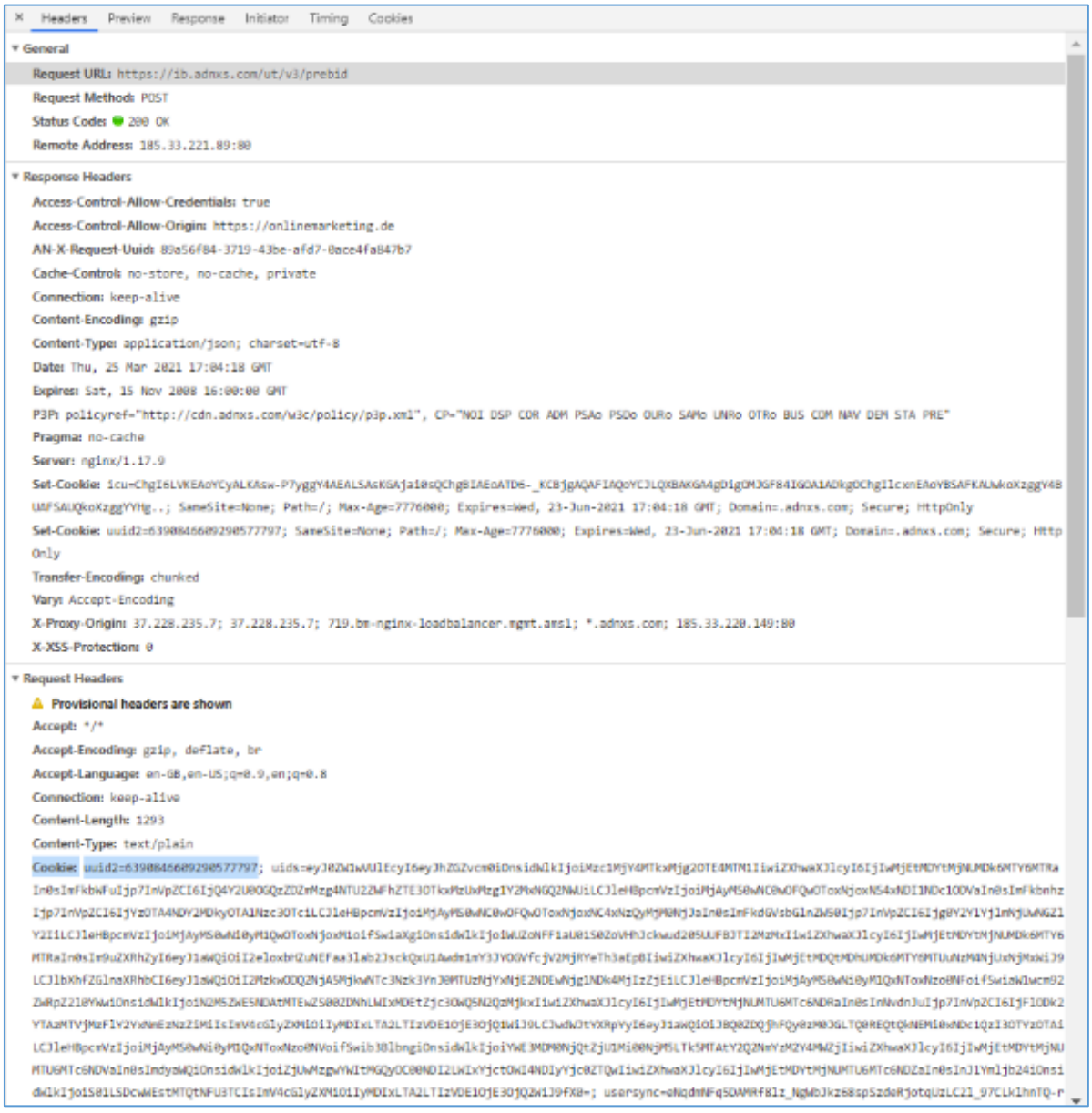
presented as **Annex K 32**

(c) Loading the following DSPs and transferring data parameters and personal data of the plaintiff relevant for the execution of the auction to them, including to the 2nd defendant:

- Criteo,
- Adscale,
- Xandr (defendant 2),
- Smartadserver,
- Adform,
- OpenX and
- other third-party providers such as NuggAdd and Adscale.



(5) Due to the integration of the 2nd defendant's tools on the 3rd defendant's website, six server requests (https://ib.adnxs.com/ut/v3/prebid) for the 2nd defendant to submit a bid request were sent out by the plaintiff's browser in the background when the 3rd defendant's website was loaded. With these server requests, the 2nd defendant was asked to send bid requests to the multitude of companies participating in its auctions.

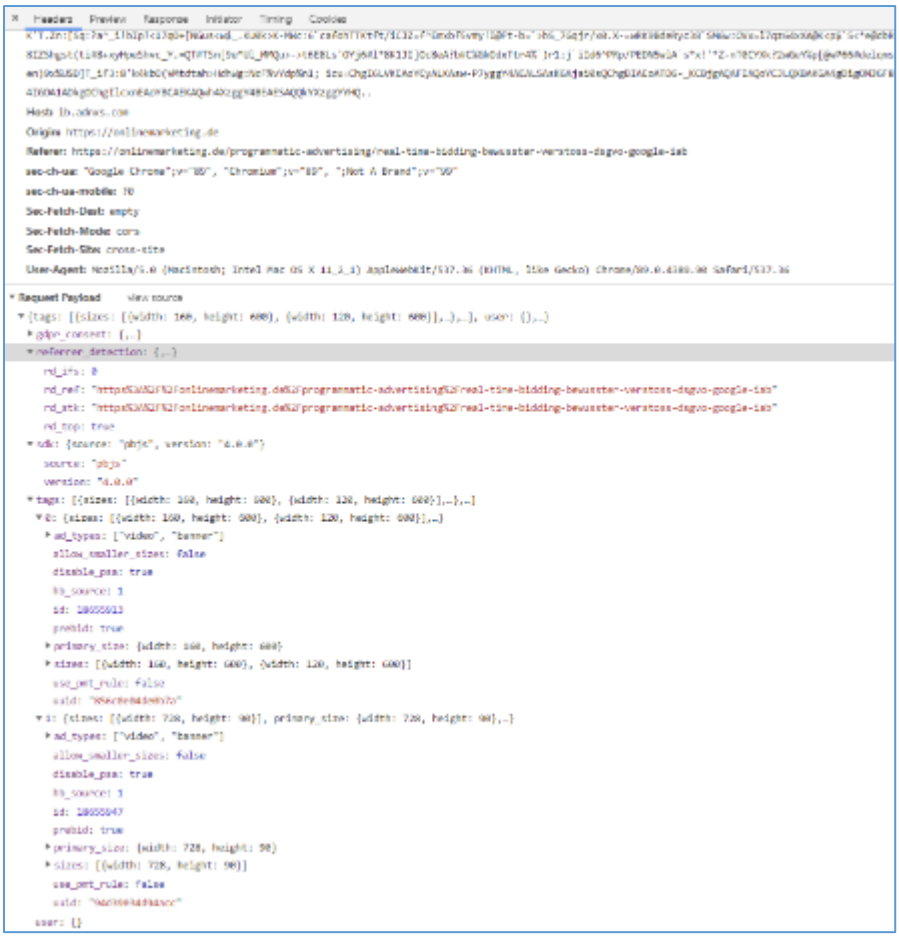


Offer of Proof: partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 indicating a server request to submit a bid request by defendant 2,

submitted as **Annex K 33**

The server request (https://ib.adnxs.com/ut/v3/prebid) of the 2nd defendant initiated by the 3rd defendant on 25 March 2021 at 5:04 p.m. (GMT+0, corresponding to 6:04 p.m. German time)

included all of the plaintiff's data parameters required to conduct a Real Time Bidding auction, such as the user ID ("uuid2"), cookie information for matching with third-party platforms (matching ID), information on the plaintiff's browser settings, parameters for the auction, as well as server information.



Offer of proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the details for the 2nd defendant's server request,)

submitted as **Annex K 34**

(6) On the occasion of the server request (https://ib.adnxs.com/ut/v3/prebid) of the 2nd defendant, personal data of the plaintiff were sent to the DSPs on the server side in the bid request. In doing so, the technical standard OpenRTB API Specification Version 2.4 of the 1st defendant was

used by the 2nd defendant on the 3rd defendant's website to carry out Real Time Bidding, as can undoubtedly be seen from the "Default Endpoint" of the 2nd defendant's server request (https://prebid.adnxs.com/pbs/v1/openrtb2/auction) specified in the programming of the 3rd defendant's website.

Offer of Proof: Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 03/25/2021 showing the details for the bid requests by the 2nd defendant,)

presented as **Annex K 35**

Defendant 2 also states that it uses defendant 1's technical standard OpenRTB API Specification

Version 2.4.

Offer of Proof: Entire Printout of defendant's Integration Guide for SSPs, Incoming Bid Requests from SSPs, as amended Feb. 5, 2021, available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed Mar. 29, 2021,

presented as **Annex K 36**

1st defendant's March 2016 technical standard "OpenRTB API Specification Version 2.4" includes both the user data parameters later specified by 1st defendant's AdCOM Specifcation v1.0 standard and content from 1st defendant's later Content Taxonomy (v2.0 since 2017) and Audience Taxonomy (v.1.0 since 2019) standards.

Offer of Proof: Entire printout of 1st defendant's Protocol Technical Specifications, OpenRTB API Specifications Version 2.4, as amended March 2016, available at: https://iabtechlab.com/wp-content/uploads/2016/04/OpenRTB-API-Specification-Version-2-4-FINAL.pdf, last accessed 03/29/2021,

presented as **Annex K 37**

Bidding requests that the 2nd defendant forwards to DSPs contain personal data of the plaintiff. The 2nd defendant itself makes examples of bid requests publicly available.

Example Bid Requests

Banner Bid Request


```
{
    "id": "3456789098765432",
    "imp": [{
        "banner": {
            "h": 300,
            "w": 750
        },
        "bidfloor": 0.0779016539,
        "bidfloorcur": "USD",
        "id": "a3f74205-6a2d-43e1-b346-693b0dad1972",
        "pmp": {
            "deals": [{
                "bidfloor": 1.03866878,
                "bidfloorcur": "USD",
                "id": "123456789"
            }],
            "private_auction": 1
        }
    }, {
        "banner": {
            "h": 300,
            "w": 750
        },
        "bidfloor": 0.0779016539,
        "bidfloorcur": "USD",
        "id": "5a123e7a-e72e-4503-913e-03fdad931de4",
        "pmp": {
            "deals": [{
                "bidfloor": 1.03866878,
                "bidfloorcur": "USD",
                "id": "654321234"
```

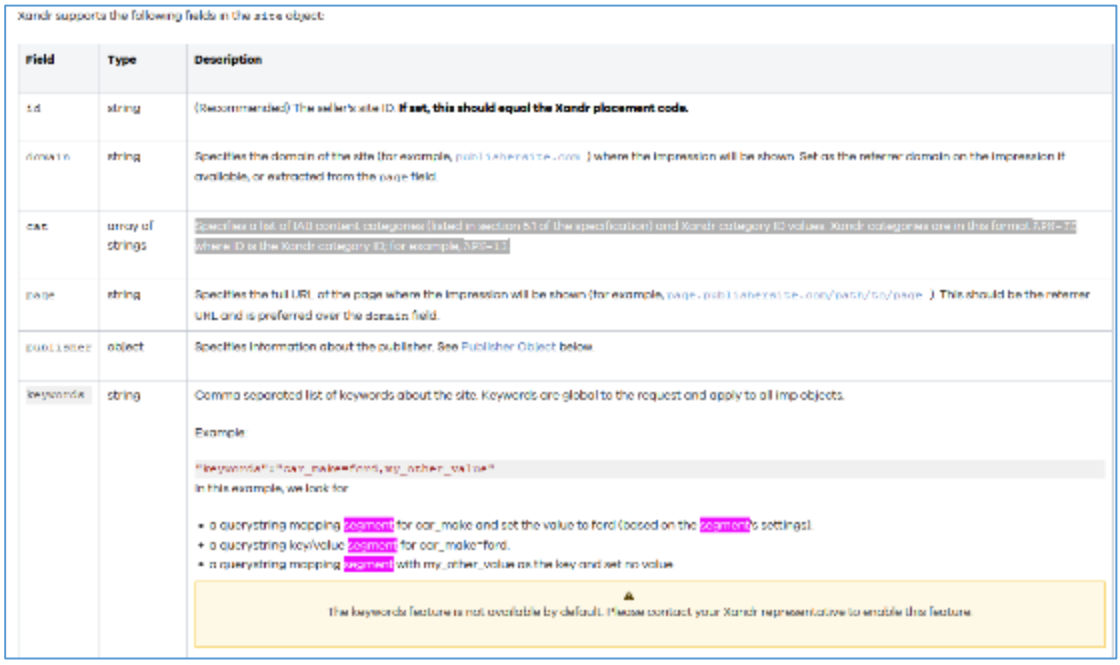


```
            }],
            "private_auction": 1
        }

    }, {
        "banner": {
            "h": 60,
            "w": 468
        },
        "bidfloor": 0.0779016539,
        "bidfloorcur": "USD",
        "id": "312305dd-6643-4bfd-8ee6-4b14f8755dad",
        "pmp": {
            "deals": [{
                "bidfloor": 1.03866878,
                "bidfloorcur": "USD",
                "id": "432123456"
            }],
            "private_auction": 1
        }
    }, {
        "banner": {
            "h": 250,
            "w": 970
        },
        "bidfloor": 0.0779016539,
        "bidfloorcur": "USD",
        "id": "1123a57b-464e-4b6d-87ae-89f501dadfb9",
        "pmp": {
            "deals": [{
                "bidfloor": 1.03866878,
                "bidfloorcur": "USD",
                "id": "543234567"
            }],
            "private_auction": 1
```

The sample bid requests of the 2nd defendant can be taken from the overall printout of the 2nd defendant's integration guide for SSPs, Incoming Bid Requests from SSPs, as amended on 05.02.2021 (already submitted as **Annex K 36,** available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed on 29.03.2021).

In addition to the sample bidding requests, the 2nd defendant states that it also uses categories from the 1st defendant's technical standards Content Taxonomy (see A. II. 2. c), p. 26, and A. IV. 2. b) bb), p. 105) and Audience Taxonomy (see A. II. 2. d), p. 27, and A. IV. 2. b) cc), p. 110) in bidding requests.



Xandr supports the following fields in the site object:

Field	Type	Description
id	string	(Recommended) The seller's site ID. **If set, this should equal the Xandr placement code.**
domain	string	Specifies the domain of the site (for example, publishersite.com) where the impression will be shown. Set as the referrer domain on the impression if available, or extracted from the page field.
cat	array of strings	Specifies a list of IAB content categories (listed in section 5.1 of the specification) and Xandr category ID values. Xandr categories are in the format XPR-ID, where ID is the Xandr category ID; for example, XPR-12.
page	string	Specifies the full URL of the page where the impression will be shown (for example, page.publishersite.com/path/to/page). This should be the referrer URL and is preferred over the domain field.
publisher	object	Specifies information about the publisher. See Publisher Object below.
keywords	string	Comma separated list of keywords about the site. Keywords are global to the request and apply to all imp objects. Example: "keywords":"car_make=ford,my_other_value" In this example, we look for: • a querystring mapping segment for car_make and set the value to ford (based on the segment's settings). • a querystring key/value segment for car_make=ford. • a querystring mapping segment with my_other_value as the key and set no value. ⚠ The keywords feature is not available by default. Please contact your Xandr representative to enable this feature.

Offer of Proof: Partial Printout of defendant 2's Integration Guide for SSPs, Incoming Bid Requests from SSPs, as amended Feb. 5, 2021, available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed Mar. 25, 2021,

presented as **Annex K 38**

Corresponding bid requests were also sent by the 2nd defendant when visiting the 3rd defendant's website to a high number of DSPs that cannot be precisely quantified by the plaintiff. This is evidenced by the server response that the 2nd defendant sent to the 3rd defendant in response to the server request (https://ib.adnxs.com/ut/v3/prebid), which was initiated by the 3rd defendant. In the server response of the 2nd defendant, all auction-relevant parameters for the advertising space in question on the 3rd defendant's website and the collection of the plaintiff's cookie information are transferred to the 3rd defendant.

This information transferred by the 2nd defendant shows that the following personal data of the plaintiff were forwarded to all DSPs that were connected to 2nd defendant:

- IP address ("ip");

- User ID ("user": "id");
- Sex ("gender");
- Date of birth ("yob");
- Information about the browser and operating system ("ua");
- Location of the terminal device ("geo");
- Residence ("city");
- Location of the "home" ("geo", "home base");
- Current location of the user ("lat", "lon" or IP address);
- additional stored data fields ("ext");
- Categories from the Content Taxonomy ("cat" = version 2.0, "bcat" = version 1.0): interests of the plaintiff, based on which websites he or she visits (this may include very sensitive personal characteristics such as religion, political views, sexuality or state of health, for more details see point A. IV. 2. b) bb), p. 105;
- Audience Taxonomy Categories ("segments"): "segments" into which Plaintiff has been classified (classification is based on profile data obtained either from Advertising Exchange itself or from third parties, which may include highly sensitive information about religion, political views, sexuality, or health - for example, Defendant 1's list includes the segment "Cancer," described in more detail in A. IV. 2. b) cc), p. 110
- a personal identifier of the plaintiff used by a DSP and an advertising exchange ("publisher");
- Plaintiff's equipment characteristics, including:
    - Height, width and aspect ratio of the screen ("banner");
    - Device manufacturer, model, version ("ua");
    - Operating system including version ("ua");
    - Browser software and version ("ua");
    - Language ("ua").

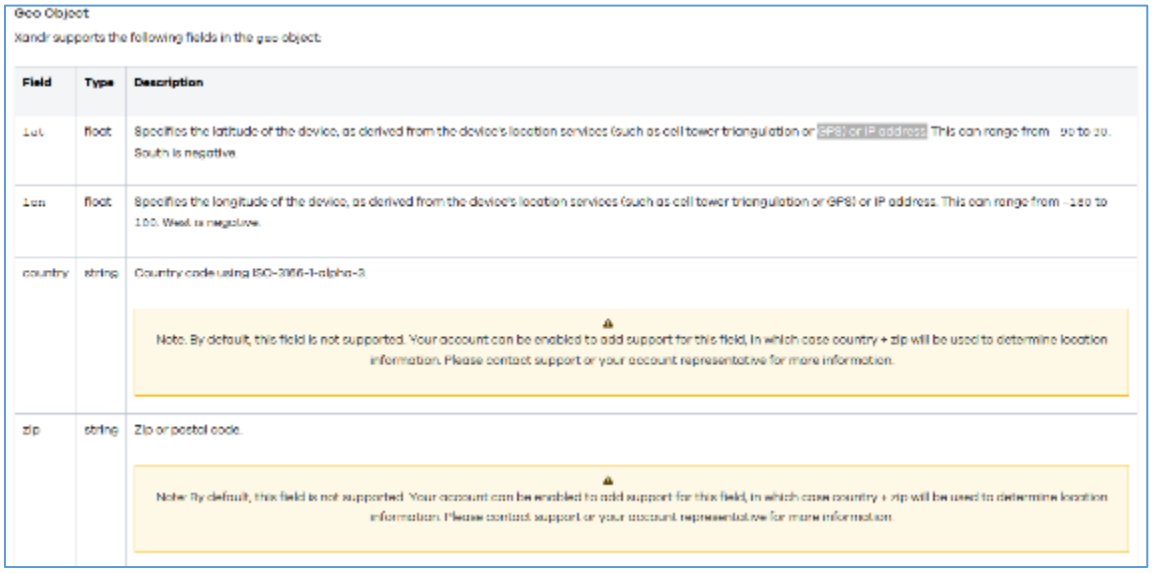
Xandr supports the following fields in the `user` object:

Field	Type	Description
`id`	string	The seller's unique ID for this user. Used for seller debugging purposes only.
`buyeruid`	string	The Xandr unique ID of this user. If set, this value will overwrite the `cookieuid` value.
`yob`	integer	Specifies the year of birth as a 4-digit integer. Omitted when sent to buyers if unknown or value set to `0`.
`gender`	string	Specifies the gender. Set to `null` if unknown. Omitted when sent to buyers if unknown. • `M`: male • `F`: female • `O`: other
`customdata`	string	A properly encoded string that can contain an Xandr user ID. Will be ignored if `buyeruid` is set.
`keywords`	string	Comma separated list of keywords about the user. Keywords are global to the request and apply to all `imp` objects. Example: `"keywords":"car_make=ford,my_other_value"` In this example, we look for: • a querystring mapping segment for car_make and set the value to ford (based on the segment's settings). • a querystring key/value segment for car_make=ford. • a querystring mapping segment with my_other_value as the key and set no value. ⚠ The keywords feature is not available by default. Please contact your Xandr representative to enable this feature.
`geo`	object	Location of the user's home base defined by a Geo object. This is not necessarily their current location. ⚠ Note: By default, this field is not supported. Please contact support or your account representative for more information.

Device Object

Xandr supports the following fields in the `device` object. Note that the device IDs in this object should override any device IDs in the Bid Request Extension Object.

Field	Type	Description
`ua`	string	(Recommended) Specifies the user agent string from the browser. User agent often identifies such information as the application, operating system, and software vendor acting on behalf of the user, e.g. `"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.0.4) Gecko/2008102920 Firefox/3.0.4"`.
`geo`	object	Specifies the location of the device, as derived from the device's location services (such as cell tower triangulation or GPS) or IP address. See Geo Object for details.
`dnt`	integer	Specifies the Do Not Track setting. • `0`: Do Not Track is set to false in browser (tracking is allowed) • `1`: Do Not Track is set to true in browser (user has opted out of tracking)
`ip`	string	Specifies the IPv4 address closest to the device. Omitted when sent to buyers if seller visibility settings prohibit sharing.
`ipv6`	string	Specifies the IPv6 address closest to the device. Used only for geolocation for buyer targeting.
`devicetype`	integer	Specifies the type of device, using IAB values. • `1`: Mobile/Tablet • `2`: Personal Computer • `3`: Connected TV • `4`: Phone • `5`: Tablet • `6`: Connected Device • `7`: Set Top Box



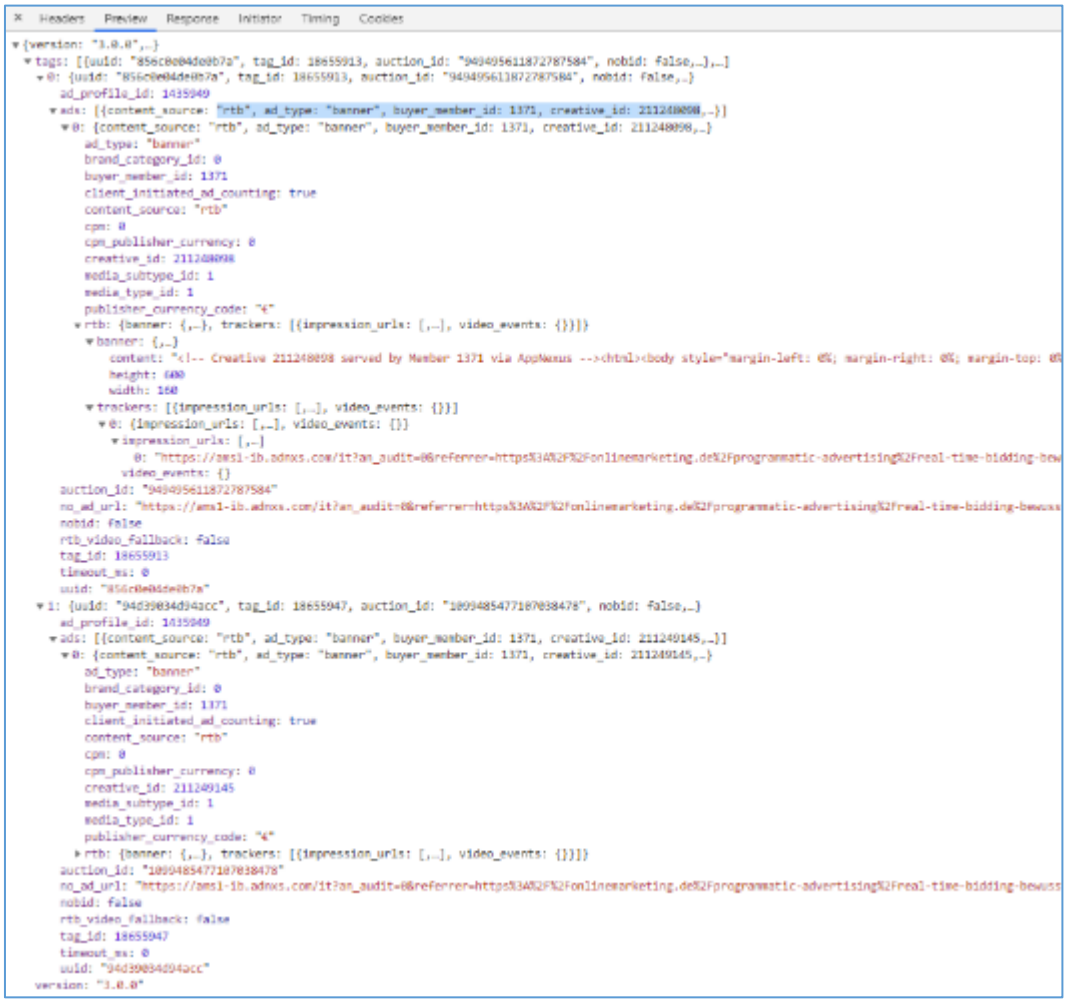
Geo Object

Xandr supports the following fields in the geo object:

Field	Type	Description
lat	float	Specifies the latitude of the device, as derived from the device's location services (such as cell tower triangulation or GPS) or IP address. This can range from -90 to 90. South is negative.
lon	float	Specifies the longitude of the device, as derived from the device's location services (such as cell tower triangulation or GPS) or IP address. This can range from -180 to 180. West is negative.
country	string	Country code using ISO-3166-1-alpha-3. Note: By default, this field is not supported. Your account can be enabled to add support for this field, in which case country + zip will be used to determine location information. Please contact support or your account representative for more information.
zip	string	Zip or postal code. Note: By default, this field is not supported. Your account can be enabled to add support for this field, in which case country + zip will be used to determine location information. Please contact support or your account representative for more information.

The individual data fields of a bid request of the 2nd defendant can be taken from the overall printout of the 2nd defendant's integration guide for SSPs, “Incoming Bid Requests from SSPs”, as amended on 5 February 2021 (already submitted as **Annex K 36,** available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html**,** last accessed on 29 March 2021).

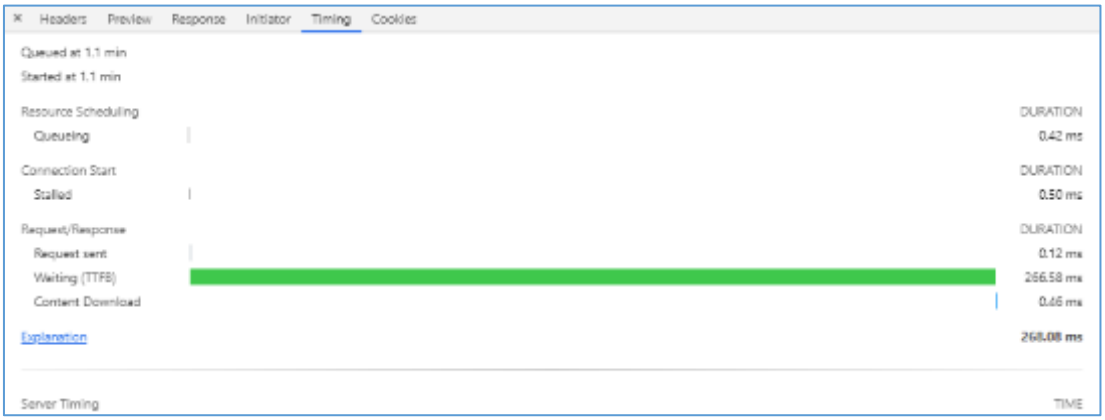
(7) The server responses of the 2nd defendant to the server requests initiated by the 3rd defendant (https://ib.adnxs.com/ut/v3/prebid) contain multiple clear references to Real Time Bidding ("content_source": "rtb", "rtb_video_fallback", "rtb", "banner") and information on the auction ("AuctionsID", "Buyer-Member ID", i. e. winner of the auction), Creative-ID, the fee paid (CMP = Cost per Mile), and the currency paid ("publisher_currency_code", "€"). i.e. winner of the auction), Creative-ID, the paid fee (CMP = Cost per Mile), as well as the paid currency ("publisher_currency_code","€").



Offer of Proof: Partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing defendant 2's server response with details of the Real Time Bidding auction conducted,

submitted as **Annex K 39**

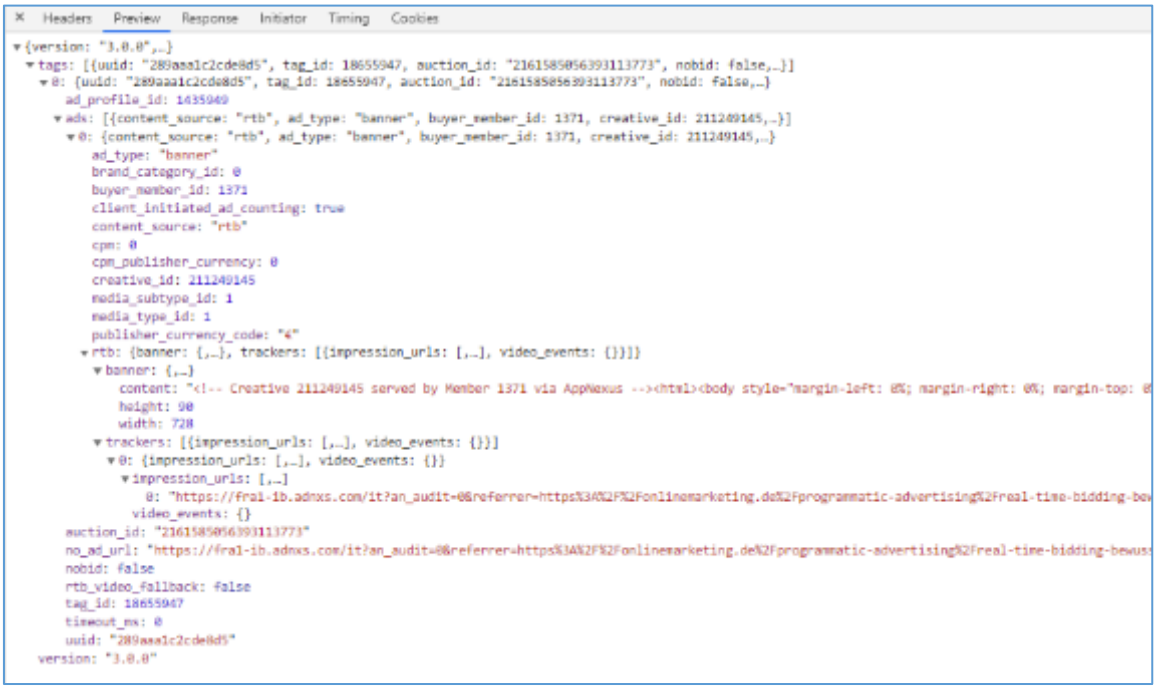
The duration of the auction on 25.03.2021 at 17:04 (GMT+0, equivalent to 18:04 German time) with the disclosure of the plaintiff's personal data to an unspecified number of DSPs was 268.08 milliseconds.



Offer of Proof: Partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing the length of time between server request and server response of defendant 2's with details of the Real Time Bidding auction conducted,

submitted as **annex K 40**

In doing so, defendant 2 sent several server responses to defendant 3, whereby it was observed that server responses differed between several page views because the "auction_id" changed, as did the the winners of the auction (Buyer-Member ID, Creative-ID), and so-called "nobid" reponses were returned if no bid was made in the auctions.



Offer of Proof: Partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing defendant 2's server response with amended details of the Real Time Bidding auction conducted,

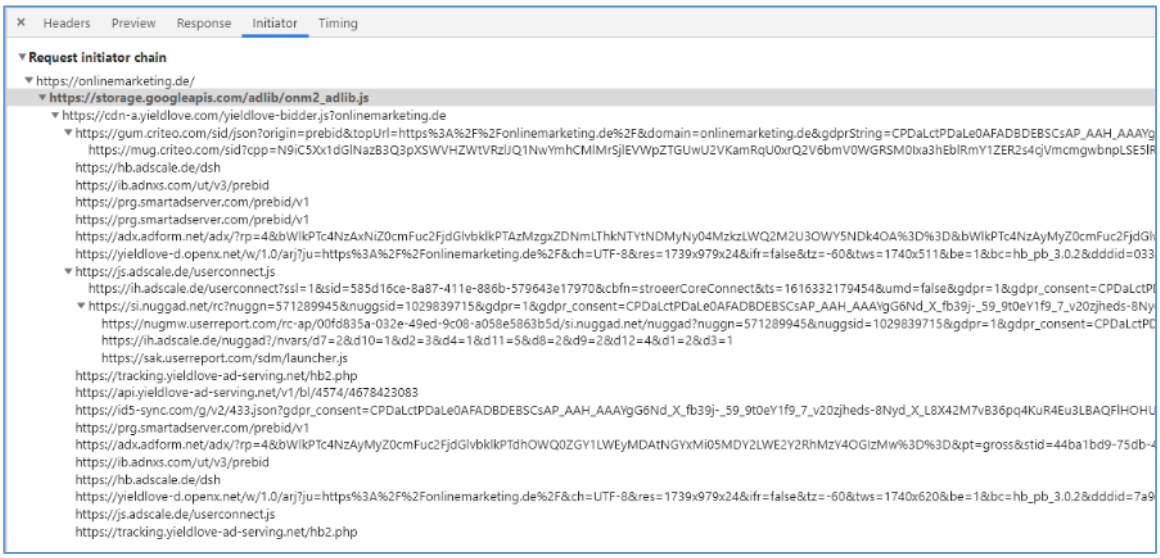
submitted as **Annex K 41**

It is thus established that personal data of the plaintiff were processed and sent by the 2nd defendant to an unspecified number of DSPs for the purpose of conducting a real-time auction of available advertising space on the 3rd defendant's website, using the 1st defendant's technical standard.

b) Real-time auctioning via OpenRTB API Specification Version 2.5

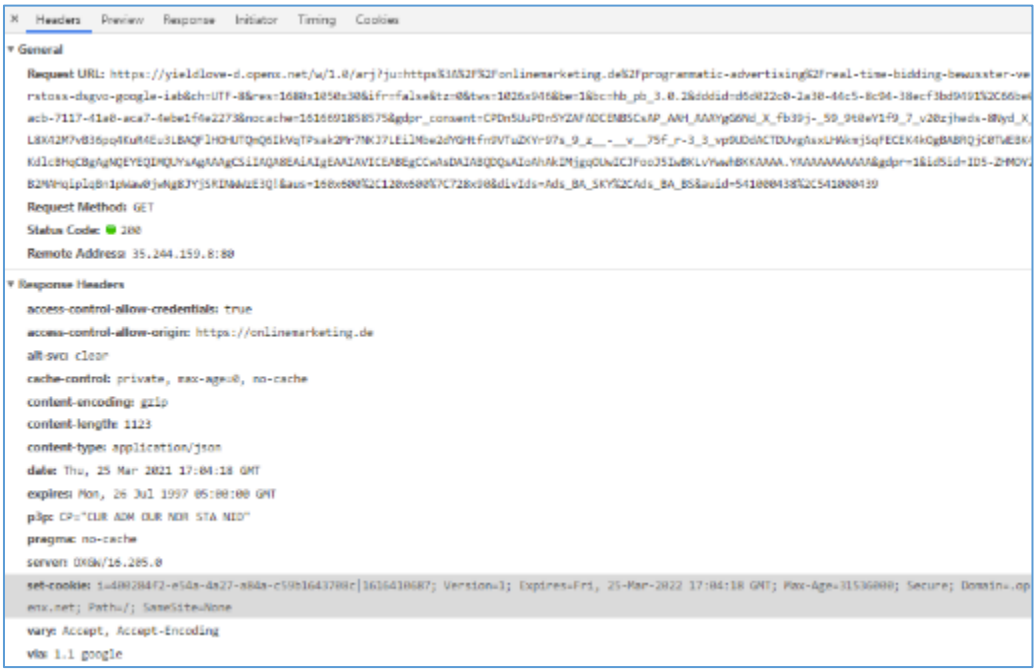
(1) When the article about the plaintiff was loaded on the website of the 3rd defendant (https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten), a header bidding (cf. point A. II. 3. a) (1), p. 29 server request

(https://yieldlove-d.openx.net/w/1.0/arj) was sent to OpenX in order to carry out real time bidding. Open X (OpenX Technologies, Inc., 888 E Walnut St., Pasadena, CA 91191) is another online advertising exchange.



The server requests triggered by the 3rd defendant followed the same pattern as the 2nd defendant (see point A. II. 3. a. (1), p. 29).

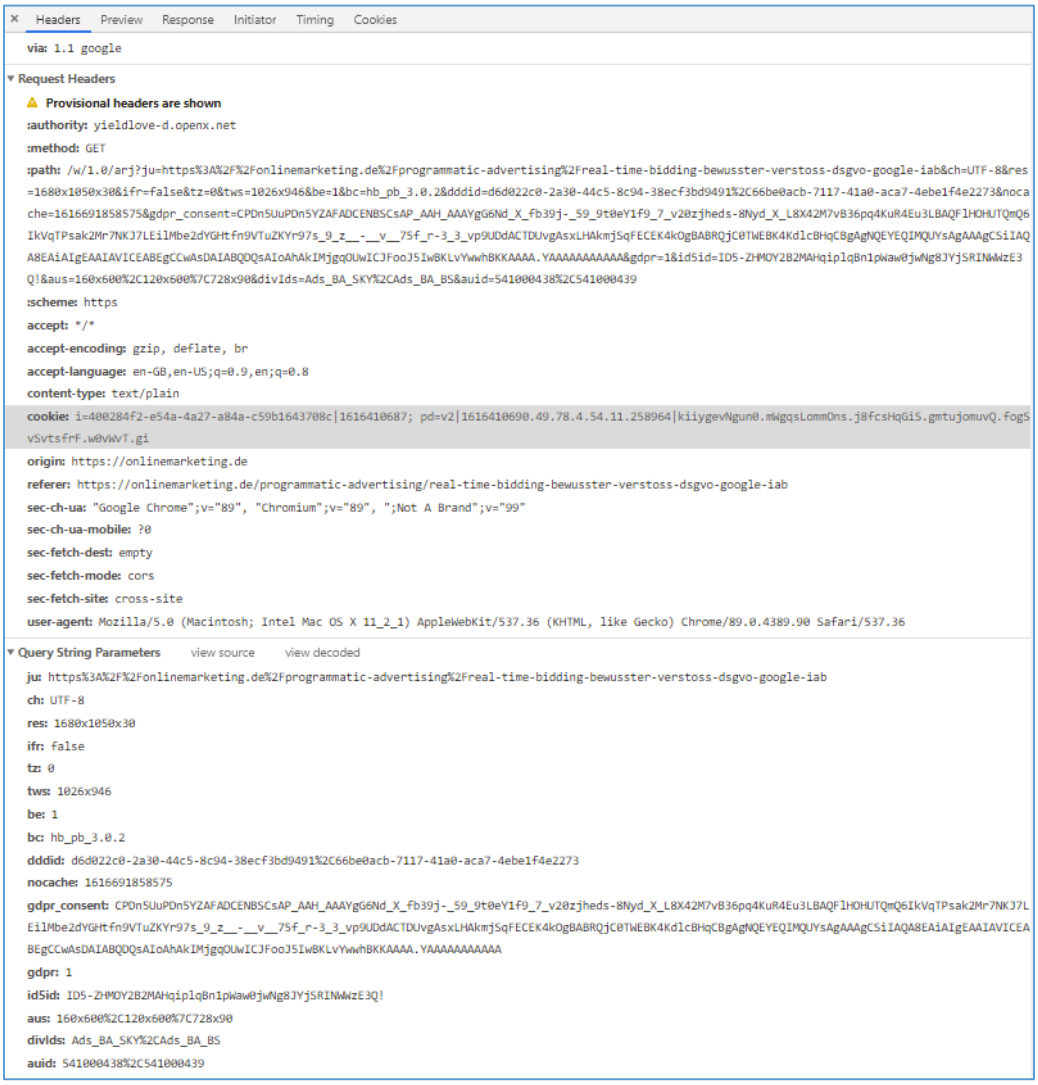
The 3rd defendant initiated the server request (https://yieldlove-d.openx.net/w/1.0/arj) to the online advertising exchange OpenX on 25.03.2021 at 17:04 (GMT+0, corresponding to 18:04 German time) due to code in the source code of the 3rd defendant's website.



Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) using OpenX,

submitted as **Annex K 42**

The server request (https://yieldlove-d.openx.net/w/1.0/arj) included plaintiff's data parameters to conduct a Real Time Bidding auction, such as the previously assigned User ID ("i") with plaintiff's unique identifier (400284f2-e54a-4a27-a84a-c59b1643708c|1616410687), cookie information, plaintiff's browser settings information, auction parameters, and server information.



Headers Preview Response Initiator Timing Cookies

via: 1.1 google

Request Headers

Provisional headers are shown

:authority: yieldlove-d.openx.net

:method: GET

:path: /w/1.0/arj?ju=https%3A%2F%2Fonlinemarketing.de%2Fprogrammatic-advertising%2Freal-time-bidding-bewusster-verstoss-dsgvo-google-iab&ch=UTF-8&res=1680x1050x30&ifr=false&tz=0&tws=1026x946&be=1&bc=hb_pb_3.0.2&dddid=d6d022c0-2a30-44c5-8c94-38ecf3bd9491%2C66be0acb-7117-41a0-aca7-4ebe1f4e2273&nocache=1616691858575&gdpr_consent=CPDn5UuPDn5YZAFADCENBSCsAP_AAH_AAAYgG6Nd_X_fb39j-_59_9t0eY1f9_7_v20zjheds-8Nyd_X_L8X42M7vB36pq4KuR4Eu3LBAQFlHOHUTQmQ6IkVqTPsak2Mr7NKJ7LEilMbe2dYGHtfn9VTuZKYr97s_9_z__-__v__75f_r-3_3_vp9UDdACTDUvgAsxLHAkmjSqFECEK4kOgBABRQjC0TWEBK4KdlcBHqCBgAgNQEYEQIMQUYsAgAAAgCSiIAQA8EAiAIgEAAIAVICEABEgCCwAsDAIABQDQsAIoAhAkIMjgqOUwICJFooJ5IwBKLvYwwhBKKAAAA.YAAAAAAAAAAA&gdpr=1&id5id=ID5-ZHMOY2B2MAHqiplqBn1pWaw0jwNg8JYjSRINWWzE3Q!&aus=160x600%2C120x600%7C728x90&divIds=Ads_BA_SKY%2CAds_BA_BS&auid=541000438%2C541000439

:scheme: https

accept: */*

accept-encoding: gzip, deflate, br

accept-language: en-GB,en-US;q=0.9,en;q=0.8

content-type: text/plain

cookie: i=400284f2-e54a-4a27-a84a-c59b1643708c|1616410687; pd=v2|1616410690.49.78.4.54.11.258964|kiiygevNgun0.mWgqsLommOns.j8fcsHqGiS.gmtujomuvQ.fogSvSvtsfrF.w0vWvT.gi

origin: https://onlinemarketing.de

referer: https://onlinemarketing.de/programmatic-advertising/real-time-bidding-bewusster-verstoss-dsgvo-google-iab

sec-ch-ua: "Google Chrome";v="89", "Chromium";v="89", ";Not A Brand";v="99"

sec-ch-ua-mobile: ?0

sec-fetch-dest: empty

sec-fetch-mode: cors

sec-fetch-site: cross-site

user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36

Query String Parameters view source view decoded

ju: https%3A%2F%2Fonlinemarketing.de%2Fprogrammatic-advertising%2Freal-time-bidding-bewusster-verstoss-dsgvo-google-iab

ch: UTF-8

res: 1680x1050x30

ifr: false

tz: 0

tws: 1026x946

be: 1

bc: hb_pb_3.0.2

dddid: d6d022c0-2a30-44c5-8c94-38ecf3bd9491%2C66be0acb-7117-41a0-aca7-4ebe1f4e2273

nocache: 1616691858575

gdpr_consent: CPDn5UuPDn5YZAFADCENBSCsAP_AAH_AAAYgG6Nd_X_fb39j-_59_9t0eY1f9_7_v20zjheds-8Nyd_X_L8X42M7vB36pq4KuR4Eu3LBAQFlHOHUTQmQ6IkVqTPsak2Mr7NKJ7LEilMbe2dYGHtfn9VTuZKYr97s_9_z__-__v__75f_r-3_3_vp9UDdACTDUvgAsxLHAkmjSqFECEK4kOgBABRQjC0TWEBK4KdlcBHqCBgAgNQEYEQIMQUYsAgAAAgCSiIAQA8EAiAIgEAAIAVICEABEgCCwAsDAIABQDQsAIoAhAkIMjgqOUwICJFooJ5IwBKLvYwwhBKKAAAA.YAAAAAAAAAAA

gdpr: 1

id5id: ID5-ZHMOY2B2MAHqiplqBn1pWaw0jwNg8JYjSRINWWzE3Q!

aus: 160x600%2C120x600%7C728x90

divIds: Ads_BA_SKY%2CAds_BA_BS

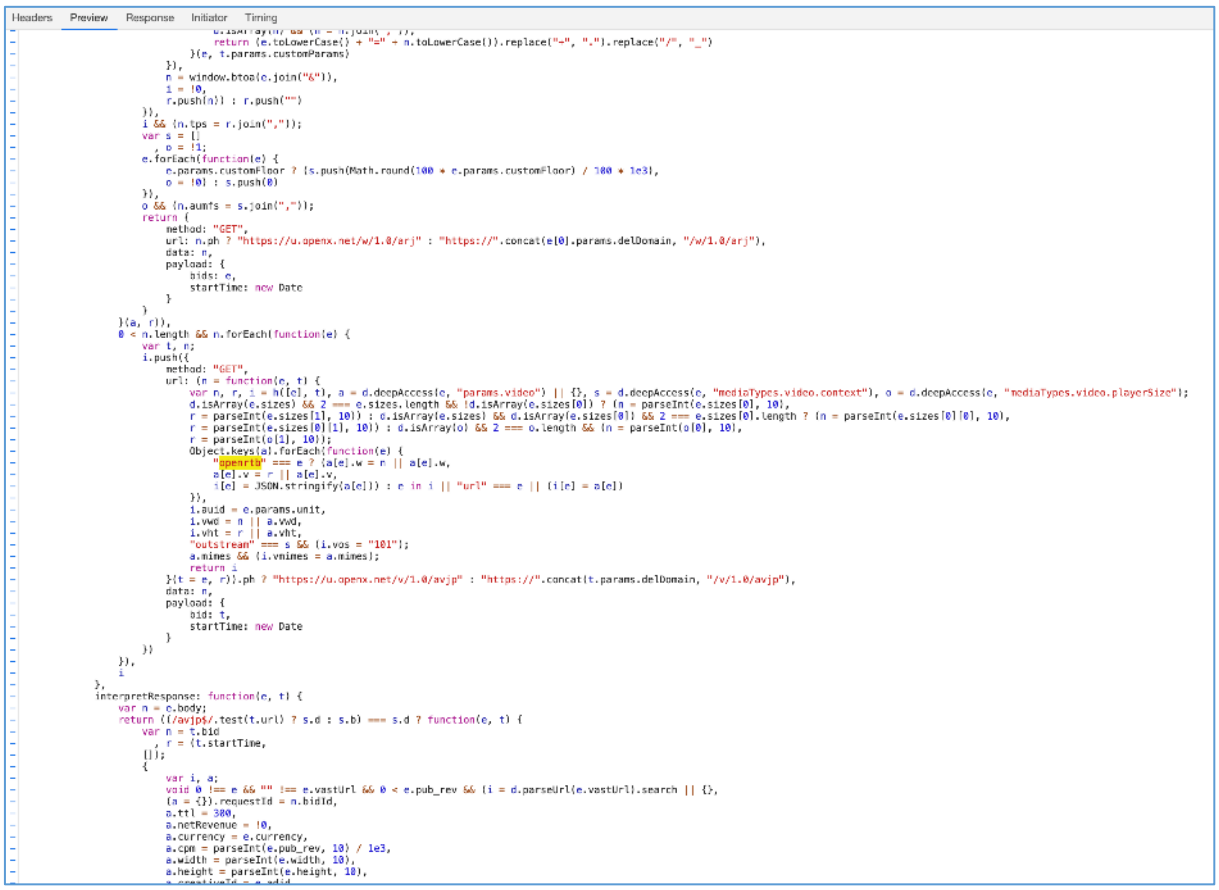
auid: 541000438%2C541000439

Offer of Proof: Partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing the server request to conduct a Real Time Bidding auction using OpenX,

presented as **Annex K 43**

(2) On the occasion of the server request (https://yieldlove-d.openx.net/w/1.0/arj) of OpenX, personal data of the plaintiff were sent on the server side in the bid request to an unspecified multitude of DSPs. In doing so, the technical standard OpenRTB of the 1st defendant was used on the website of the 3rd defendant to carry out Real Time Bidding, as can undoubtedly be seen from

the "default endpoint" of the server request (https://yieldlove-d.openx.net/w/1.0/arj) of OpenX specified in the source code of the 3rd defendant's website.



Offer of Proof: Partial printout of the website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing the server request to conduct a Real Time Bidding auction using OpenX,

presented as **Annex K 44**

According to OpenX, it uses the technical standard OpenRTB API Specification Version 2.5 of the 1st defendant.)

Offer of Proof: Partial printout of integration guide from online advertising exchange OpenX for DSPs, OpenRTB API, as amended Jan. 16, 2019, available at: https://docs.openx.com/demand-partners/ox-openrtb/#how-real-time-

bidding-works, last accessed Mar. 29, 2021,

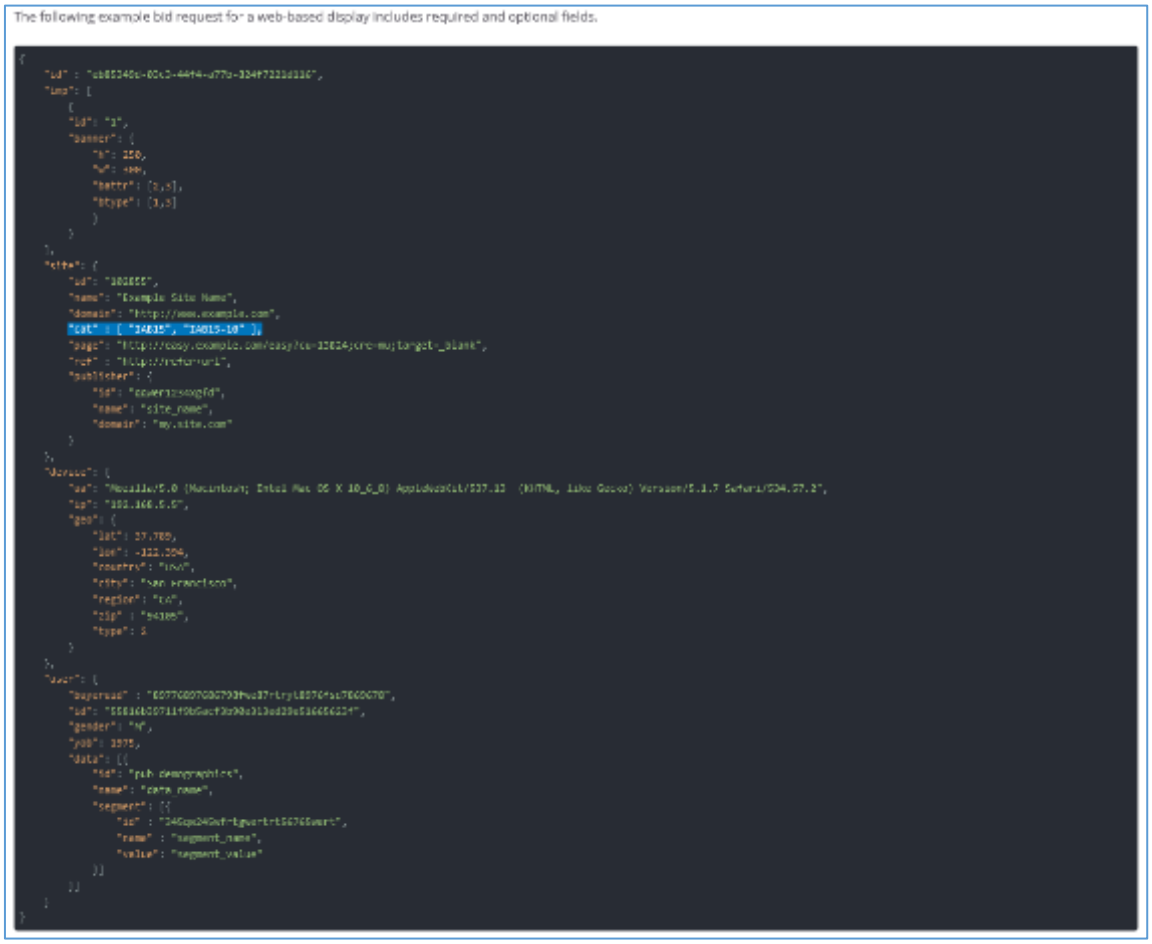
submitted as **Annex K 45**

Defendant 1's December 2016 OpenRTB API Specification Version 2.5 technical standard includes both the user data parameters later specified by defendant 1's AdCOM Specification v1.0 standard and content from defendant 1's later Content Taxonomy (v2.0 since 2017) and Audience Taxonomy (v.1.0 since 2019) standards.

Offer of Proof: Entire printout of 1st defendant's Protocol Technical Specifications, OpenRTB API Specifications Version 2.5, December 2016, available at: https://iabtechlab.com/wp-content/uploads/2016/07/OpenRTB-API-Specification-Version-2-5-FINAL.pdf, last accessed 03/23/2021,

submitted as **Annex K 46**

The bid requests that OpenX broadcasts to an unspecified number of DSPs contain the personal data of the plaintiff already listed under point A. II. 1. (p. 15). OpenX makes templates for these bid requests publicly available.



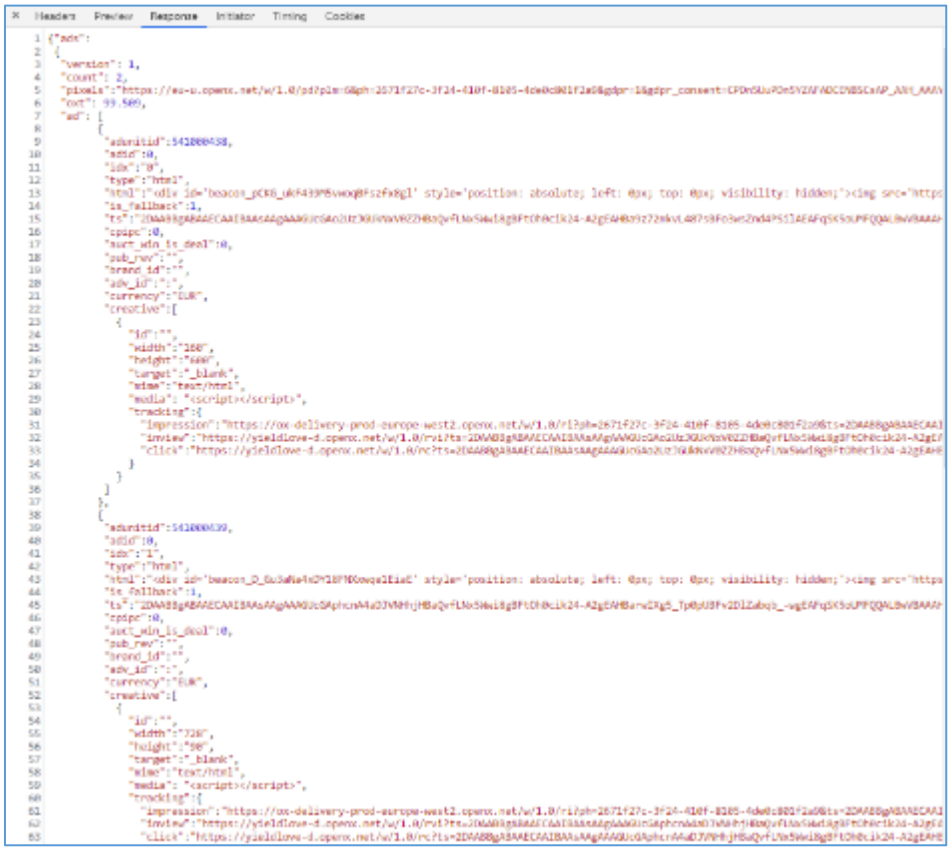
OpenX bid requests based on the technical standard OpenRTB API Specifications Version 2.5 of the 1st defendant included all or a selection of the following plaintiff's personal data:

- the location, including postcode and GPS data ("geo");
- the place of residence of the applicant ('city');
- the web content that the plaintiff views, reads or listens to on their device ("site", "app");
- plaintiff's identifiers, including
    - the user ID ("id");
    - the DSP identifier ("buyeruid");
    - a personal identifier of the plaintiff used by a DSP and an advertising exchange ("publisher");
    - unique device identifiers, such as the IMEI and MAC address, hashed in a manner in which they remain unique identification codes ("type 2");
    - the year of birth of the plaintiff ("birth");

- the sex of the plaintiff ("gender");
- the interests of the plaintiff, based on which websites he or she visits (this may include very sensitive personal characteristics such as religion, political views, sexuality or state of health, for more details see A. IV. 2. b) bb), p. 105("cat");
- the "segments" into which plaintiff has been classified (classification is based on profile data obtained either from Advertising Exchange itself or from third parties, which may include highly sensitive information about religion, political opinion, sexuality or health - for example, defendant 1's list includes the segment "cancer". Further details are described under A. IV. 2. b) cc), p. 110) ("segment");
- the device characteristics, including:
  - IP address ("ip");
  - Height, width and aspect ratio of the screen ("banner");
  - Device manufacturer, model, version ("ua");
  - Operating system including version ("ua");
  - Browser software and version ("ua");
  - Language ("ua").

(3) Corresponding bid requests were also sent by OpenX to various DSPs. This is evidenced by the server response dated 25.03.2021 that OpenX sent to the 3rd defendant, in response to the server request initiated by the 3rd defendant (https://yieldlove-d.openx.net/w/1.0/arj). In 3rd defendant's server response, all auction-relevant parameters for the advertising space in question and the plaintiff's cookie information were transferred to the 3rd defendant.

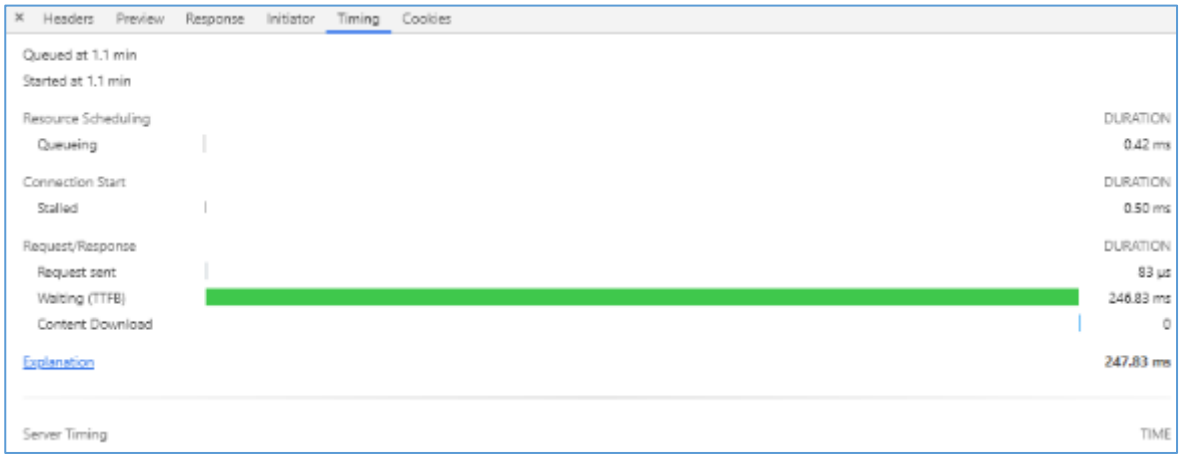
The server response from OpenX contains several clear references to Real Time Bidding and details of the auction ("auct_win_is_deal") and the currency paid ("EUR").



Offer of Proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing OpenX's server response with amended details of the Real Time Bidding auction conducted,

submitted as **Annex K 47**

The duration of the auction on 25.03.2021 at 17:04 (GMT+0, equivalent to 18:04 German time) with the disclosure of the plaintiff's personal data to an unspecified number of DSPs was 247.83 milliseconds.



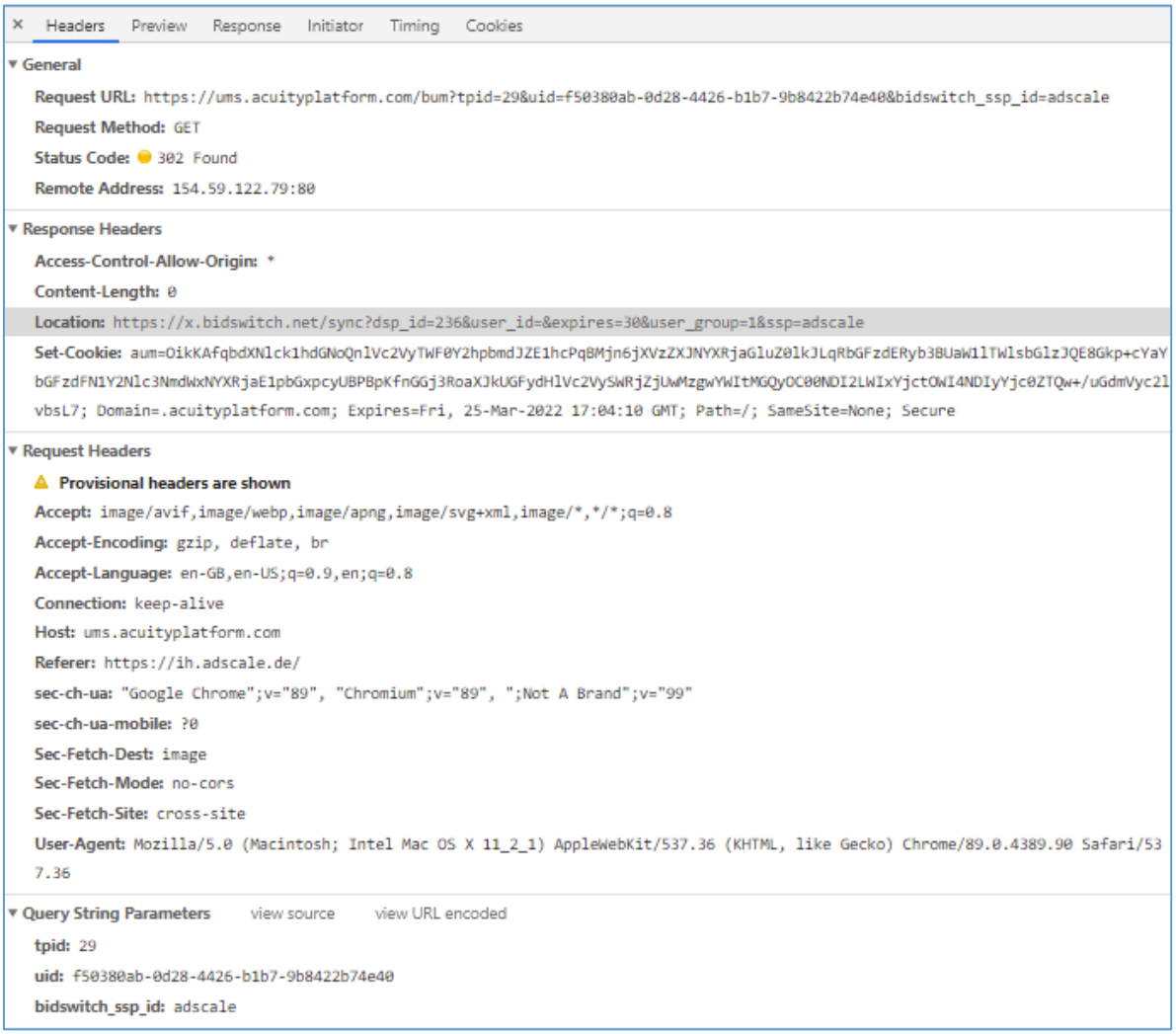
Offer of proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the duration between server request and server response from OpenX with details of the Real Time Bidding auction conducted,

presented as **Annex K 48**

c) Real-time auctioning by means of "OpenRTB Specification v3.0

When the plaintiff called up the article about the plaintiff on the website of the 3rd defendant (https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten) on 25.03.2021 at 17:04 (GMT+0, corresponding to 18:04 German time), it could also be observed that a server request (https://x.bidswitch.net/sync) was sent to BidSwitch (BidSwitch GmbH, Bahnhofstrasse 28m, 6304 Zug, Switzerland), another online advertising exchange (Advertising Exchange), in order to carry out Real Time Bidding.

(1) The server request (https://x.bidswitch.net/sync) initiated by the 3rd defendant to the online advertising exchange BidSwitch to match the plaintiff's User ID included data parameters of the plaintiff required for the execution of a Real Time Bidding auction such as the User ID ("aum"), "ssp_id=adscale" and "dsp_id=236&user". Here, "ssp" stands for Sell Side Platform and "dsp" for Demand Side Platform. It also contained cookie information, details of the plaintiff's browser settings, parameters for the auction and server information.

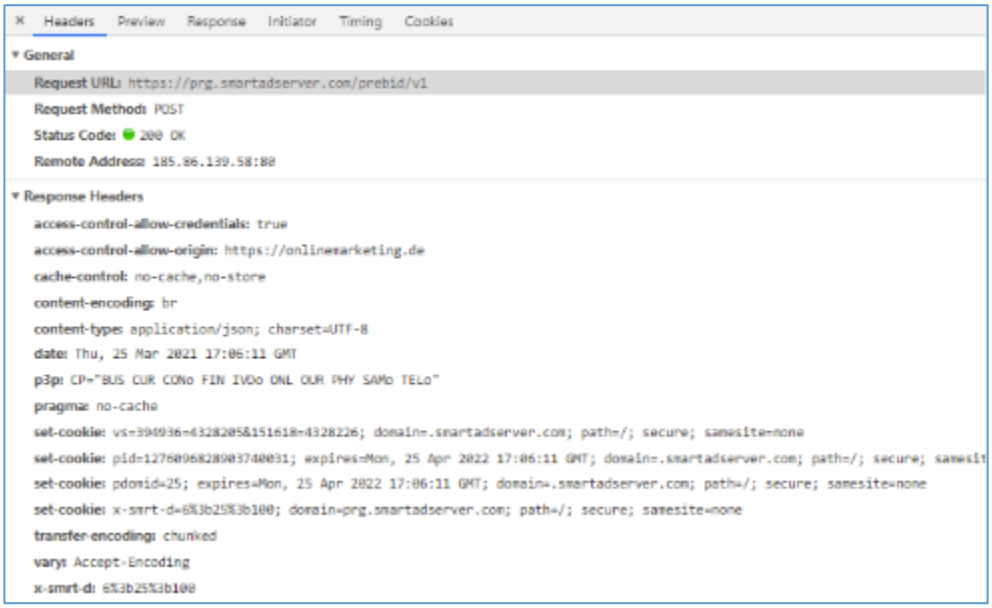


Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with BidSwitch,

submitted as **Annex K 49**

(2) Likewise, within the scope of the real-time analysis of the network connections initiated by the 3rd defendant's website, it could be observed on 15.03.2021 at 17:06 (GMT+0, corresponding to 18:06 German time) that the online advertising exchange BidSwitch was also used to forward bid requests from the SSP "SmartAdServer" (SmartAdServer SAS, 8-10 Rue Saint Paris, 75002 France) to various DSPs. The forwarding was triggered by a server request from the 3rd defendant

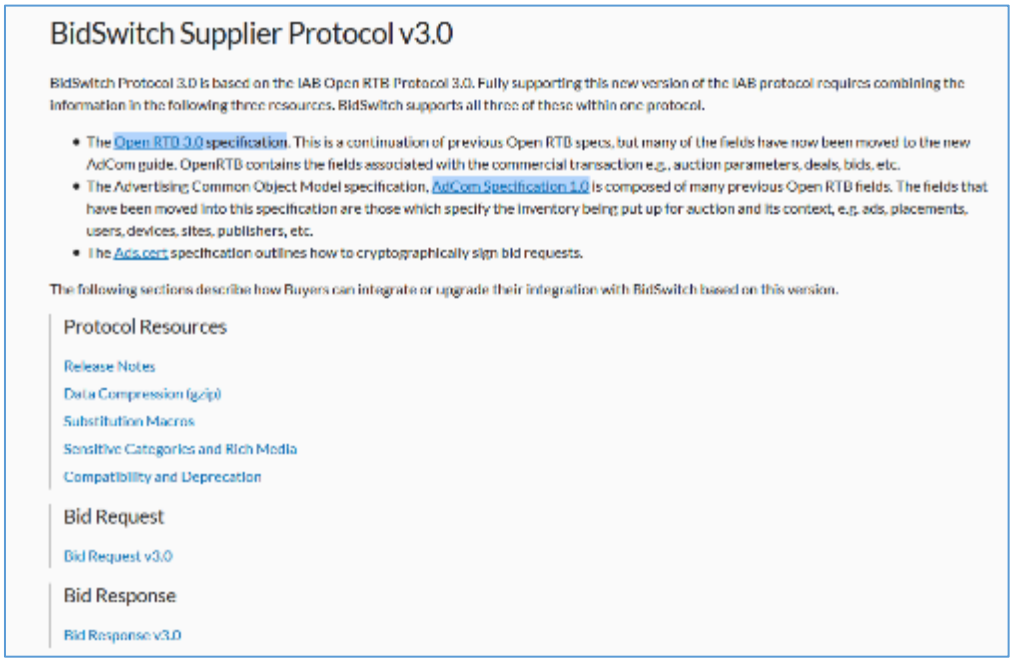
(https://prg.smartadserver.com/prebid/v1) to conduct a real time bidding auction.



Offer of proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with SmartAdServer,

presented as **Annex K 50**

(3) The server request (https://prg.smartadserver.com/prebid/v1) included personal data of the plaintiff that was sent on the server side in the bid request forwarded by BidSwitch to an unspecified number of DSPs. According to its own information, BidSwitch uses the technical standards OpenRTB Specification v3.0 (already submitted as **Annex K 16**) and AdCom Specification v1.0 (already submitted as **Annex K 24**) of the 1st defendant.)



BidSwitch Supplier Protocol v3.0

BidSwitch Protocol 3.0 is based on the IAB Open RTB Protocol 3.0. Fully supporting this new version of the IAB protocol requires combining the information in the following three resources. BidSwitch supports all three of these within one protocol.

- The Open RTB 3.0 specification. This is a continuation of previous Open RTB specs, but many of the fields have now been moved to the new AdCom guide. OpenRTB contains the fields associated with the commercial transaction e.g., auction parameters, deals, bids, etc.
- The Advertising Common Object Model specification, AdCom Specification 1.0 is composed of many previous Open RTB fields. The fields that have been moved into this specification are those which specify the inventory being put up for auction and its context, e.g. ads, placements, users, devices, sites, publishers, etc.
- The Ads.cert specification outlines how to cryptographically sign bid requests.

The following sections describe how Buyers can integrate or upgrade their integration with BidSwitch based on this version.

Protocol Resources

Release Notes
Data Compression (gzip)
Substitution Macros
Sensitive Categories and Rich Media
Compatibility and Deprecation

Bid Request

Bid Request v3.0

Bid Response

Bid Response v3.0

Offer of Proof: Partial printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/supplier-protocol.html, last accessed 03/26/2021,

presented as **Annex 51**

Offer of Proof: Entire printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/supplier-protocol.html, last accessed 03/26/2021,

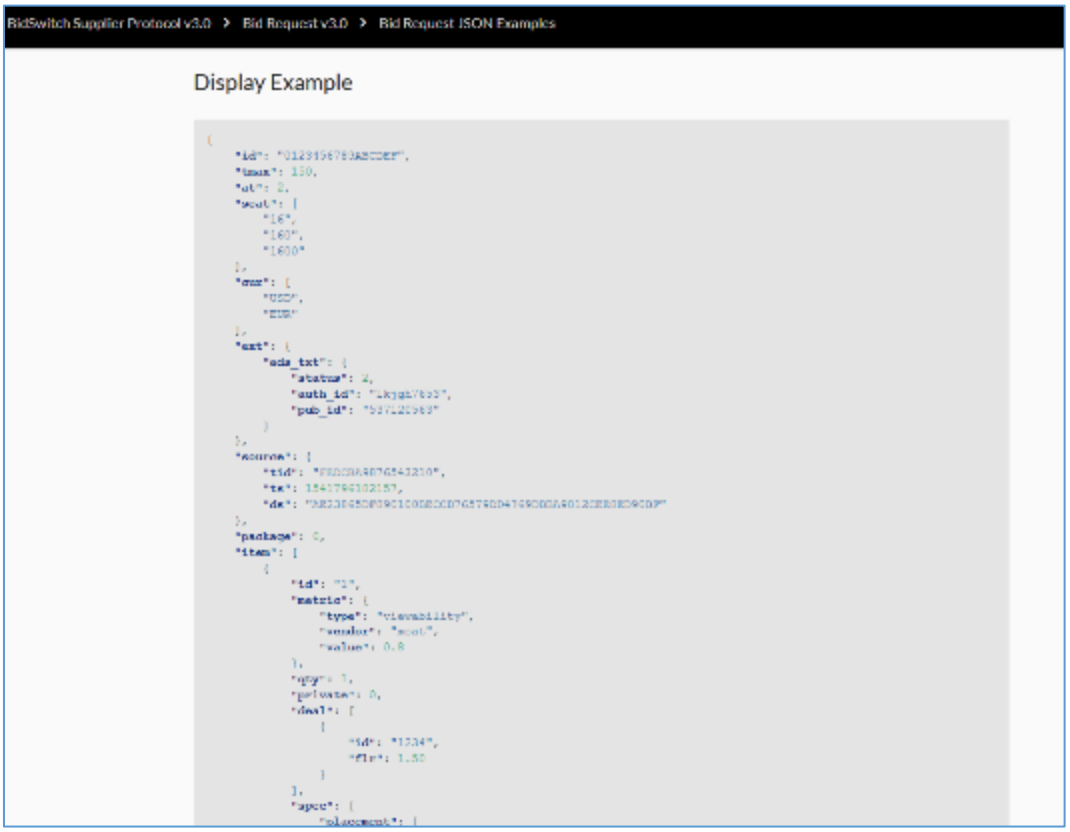
presented as **Annex 52**

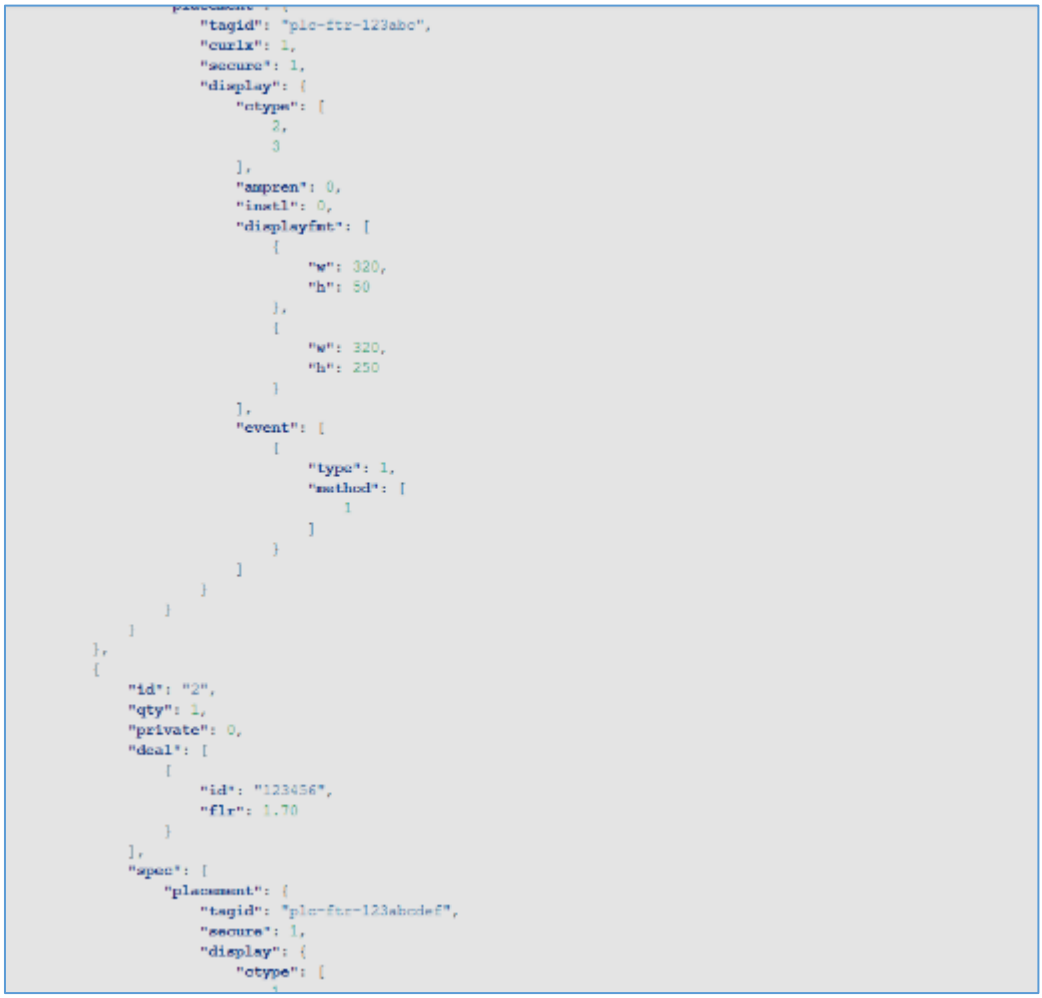
The online advertising exchange BidSwitch claims to have connected 180 SSPs and 220 DSPs and actively promotes global processing in the Real Time Bidding ecosystem. This underlines the global and mass processing of the plaintiff's personal data.

Offer of Proof: Partial printout of website at URL https://www.bidswitch.com, last accessed 03/26/2021,

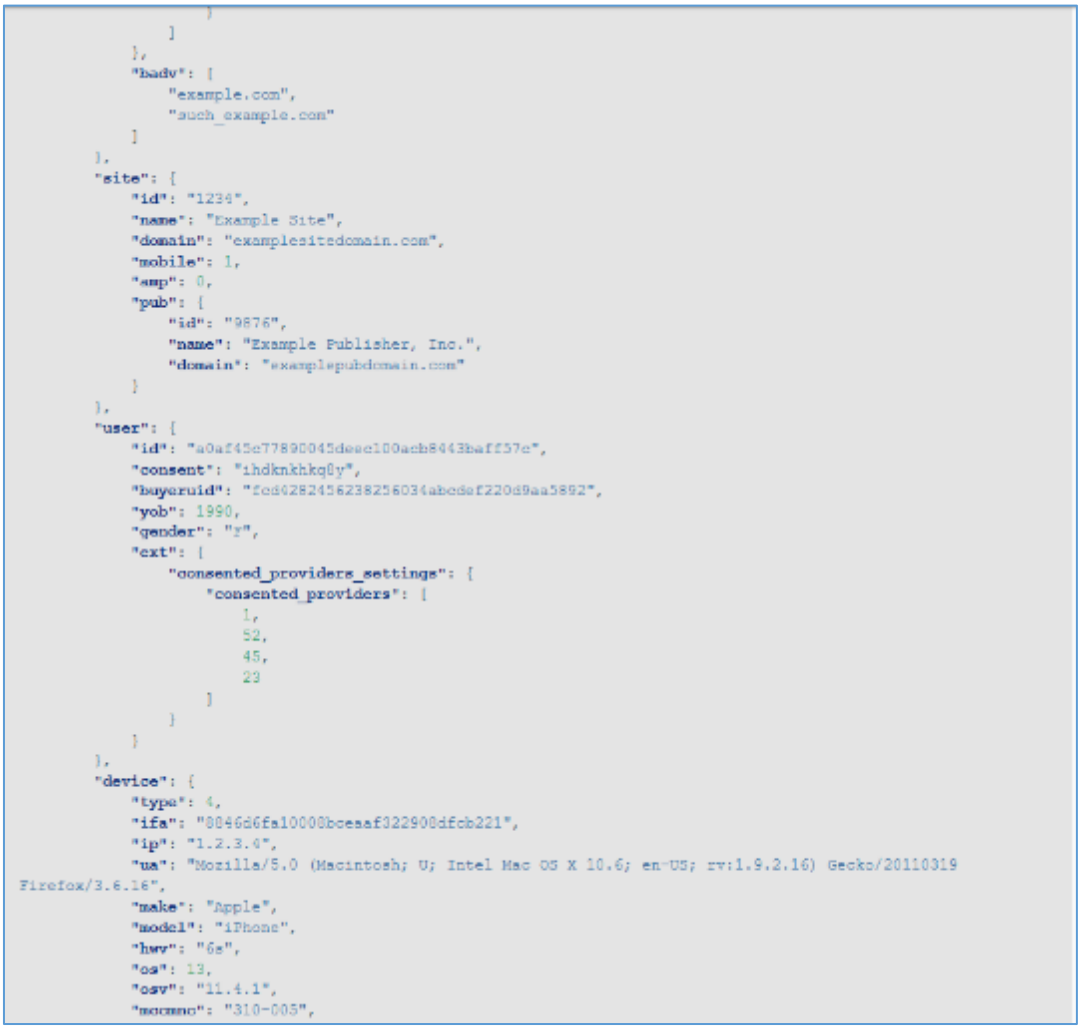
submitted as **Annex K 53**

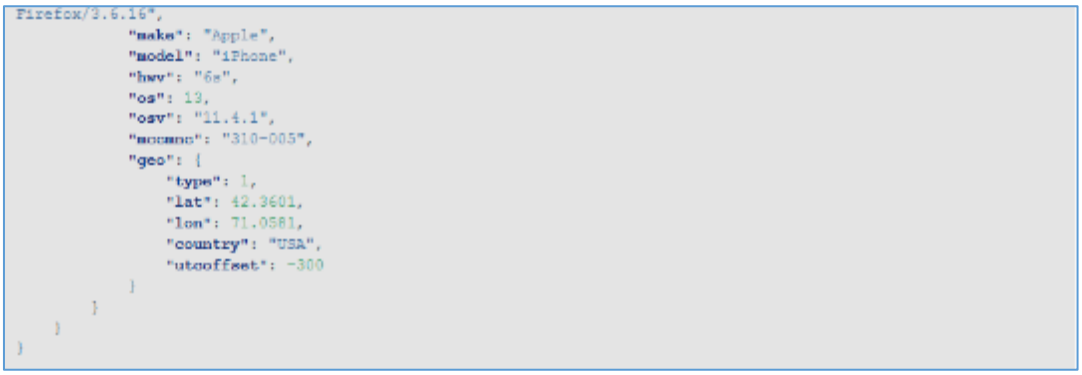
Bid requests, which BidSwitch forwards to an unspecified number of DSPs, contain personal data of the plaintiff. BidSwitch itself makes templates for bid requests publicly available.


BidSwitch Supplier Protocol v3.0 > Bid Request v3.0 > Bid Request JSON Examples
Display Example


"tagid": "plc-ftr-123abc",
"curlx": 1,
"secure": 1,
"display": {
"ctype": [
2,
3
],
"ampren": 0,
"instl": 0,
"displayfmt": [
{
"w": 320,
"h": 50
},
{
"w": 320,
"h": 250
}
],
"event": [
{
"type": 1,
"method": [
1
]
}
]
}
}
]
},
{
"id": "2",
"qty": 1,
"private": 0,
"deal": [
{
"id": "123456",
"flr": 1.70
}
],
"spec": [
"placement": {
"tagid": "plc-ftr-123abcdef",
"secure": 1,
"display": {
"ctype": [


"secure": 1,
"display": {
"ctype": [
1,
3
],
"ampren": 0,
"instl": 0,
"displayfmt": [
{
"w": 320,
"h": 50
},
{
"w": 320,
"h": 250
}
],
"event": [
{
"type": 1,
"method": [
2
]
}
]
}
}
}
}
],
"context": {
"regs": {
"gdpr": 1,
"coppa": 0
},
"restrictions": {
"cattax": 1,
"bcat": [
"IAB24",
"IAB25",
"IAB26"
],
"ext": {
"addcat": [
{
"cattax": 501,
"bcat": [
"bawl",

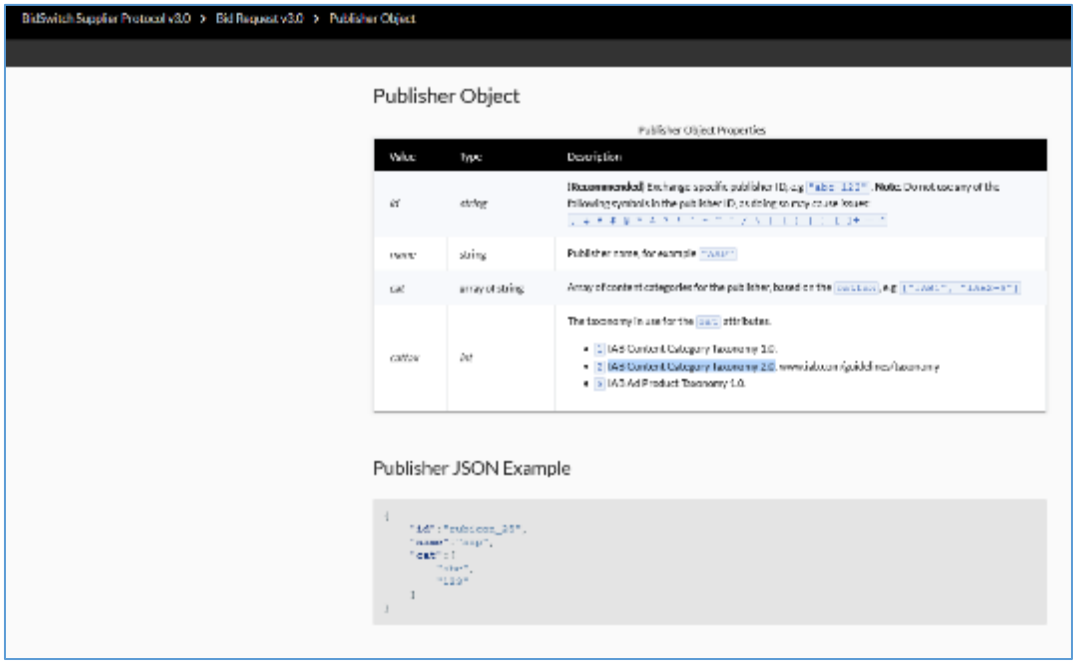




BidSwitch's sample bid requests can be found in the overall printout of the online advertising exchange BidSwitch's integration guide for DSPs, BidSwitch Supplier Protocol v3.0, (available at: https://protocol.bidswitch.com/rtb-ssp/bid-request-examples.html#display-example last accessed on 26.03.2021, already submitted as **Annex K 52**). The same sample bid requests can be

found in Appendix C of the AdCOM Specifications v1.0 standard (overall expression of the technical specifications of the 1st defendant's Protocol, AdCOM Specifications v1.0, June 2020, retrievable at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md, last accessed on 03/24/2021, already submitted as **Annex K 24**).

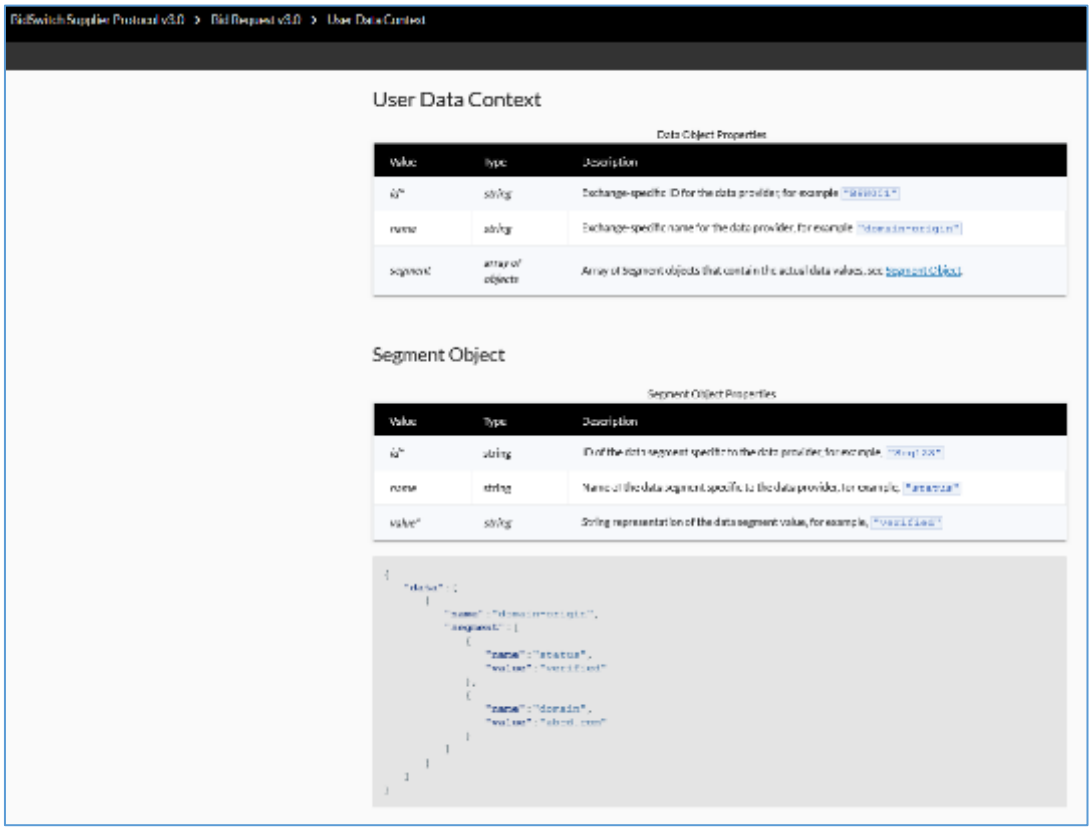
BidSwitch also states that the categories from the 1st defendant's Content Taxonomy 2.0 technical standard are included in bid requests.



Offer of Proof: Partial printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/rtb-ssp/context-pub.html, last accessed 03/26/2021,

submitted as **Annex K 54**

Furthermore, BidSwitch confirms that the categories from the 1st defendant's technical standard Audience Taxonomy are used in bid requests for the use of existing segments about the user, i.e. the previously recorded interests.



Offer of Proof: Partial printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/rtb-ssp/context-data.html, last accessed 03/26/2021,

submitted as **Annex K 55**

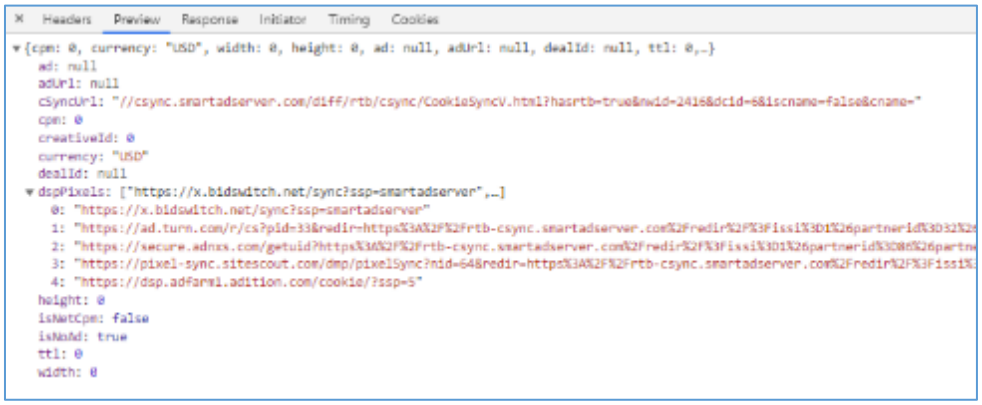
The following personal data of the plaintiff were processed in BidSwitch bid requests, based on the technical standard OpenRTB Specifications 3.0 and AdCom Specification v1.0 of the 1st defendant:

- the location, including postcode and GPS data ("geo");
- the place of residence of the applicant ('city');
- the web content that the plaintiff views, reads or listens to on their device ("site");
- plaintiff's identifiers, including
    - the user ID ("id");
    - the DSP identifier ("buyeruid");

- a personal identifier of the plaintiff used by a DSP and an advertising exchange ("publisher");
- the year of birth of the plaintiff ("birth");
- of the sex of the plaintiff person ("gender");
- the interests of the plaintiff, based on which websites he or she visits (this may include very sensitive personal characteristics such as religion, political views, sexuality or state of health, for more details see A. IV. 2. b) bb), p. 105("cat");
- "segments" into which plaintiff has been classified (classification is based on profile data obtained either from Advertising Exchange itself or from third parties, which may include highly sensitive information about religion, political opinion, sexuality, or health - for example, defendant 1's list includes the segment "cancer," described in more detail in A. IV. 2. b) cc), p. 110("segment"));
- Device features, including:
  - IP address ("ip");
  - Height, width and aspect ratio of the screen ("banner");
  - Device manufacturer, model, version ("ua");
  - Operating system including version ("ua");
  - Browser software and version ("ua");
  - Language ("ua").

(4) Corresponding bid requests were also sent by BidSwitch to various DSPs. This is evidenced by the server response dated 25.03.2021, which was sent to the 3rd defendant in response to the server request initiated by the 3rd defendant (https://prg.smartadserver.com/prebid/v1). In the server response, all auction-relevant parameters for the advertising space in question and the collection of the plaintiff's cookie information are transferred to the 3rd defendant.

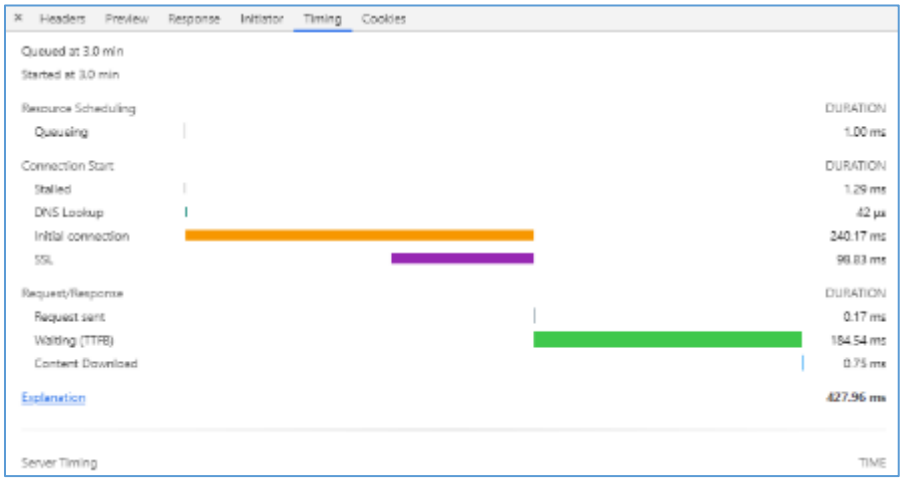
The server response contains multiple clear references to Real Time Bidding and details of the auction ("cpm", "creativeId"), the currency paid ("currency", "USD"), the advertising medium delivered ("ad") and image pixels used from SSPs ("dspPixels").



Offer of proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the server response from SmartAdServer via BidSwitch with details of the Real Time Bidding auction conducted,

submitted as **Annex K 56**

The duration of the auction on 25.03.2021 at 17:06 (GMT+0, equivalent to 18:06 German time) with the disclosure of the plaintiff's personal data to an unspecified number of DSPs was 427.96 milliseconds.



Offer of proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25.03.2021 showing the duration between server request and server response from SmartAdServer with details of the Real Time

Bidding auction conducted via BidSwitch,

presented as **Annex K 57**

4. Lack of technical and organizational measures to ensure security in OpenRTB

The system OpenRTB of the defendant 1 is already insecure from the basic structure. The insecurity is inherent in the data processing operations under OpenRTB and follows from the fundamental design of the system.

a) the extent of the data processing operations

Elizabeth Denham, head of the UK's Information Commissioner's Office (ICO), said in a report on industry practices:

> *"[...] one visit to a website, prompting one auction among advertisers, can result in a person's personal data[5] being seen by hundreds of organisations, in ways that suggest data protection rules have not been sufficiently considered. [...]".*

Offer of proof: Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019, p. 4, available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, last accessed 10 February 2021,

presented as **Annex K 58**

This description underestimates the true scale by a factor of 10: Within a single OpenRTB auction, several advertising exchanges such as the 2nd defendant may be involved. This so called "header bidding" leads to each Advertising Exchange broadcasting a bid request to up to hundreds or thousands of companies to auction a single advertising space is auctioned.

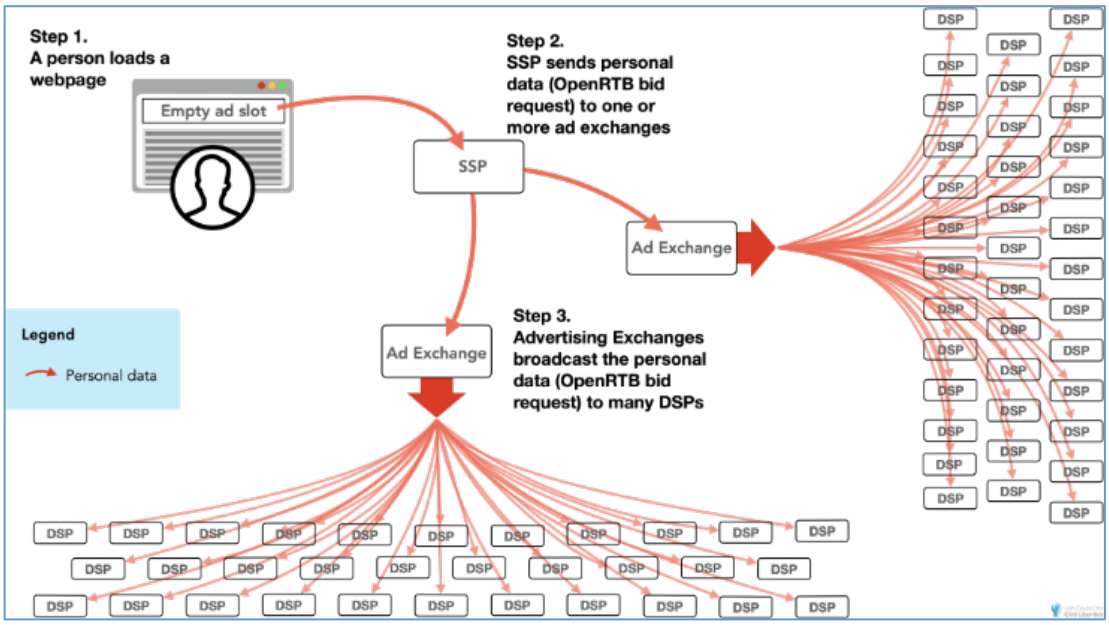
The 2nd defendant states that 1,647 companies can receive a bid request from it (cf. printout of the list of affiliated third parties of the 2nd defendant dated 12.01.2021, available at https://docs.xandr.com/bundle/service-policies/page/third-party-

providers.html#ThirdPartyProviders-Ad-serverPartners, last accessed on 24.03.2021, already submitted as **Annex K 13**).

As a result, even very small DSPs receive a large number of bid requests. In 2018, the French data protection regulator (Commission Nationale de l'informatique et des Libertés, CNIL) revealed that a single DSP called Vectaury collected bid requests from OpenRTB from 68,623,023 individuals in just one year [CNIL, Décision n° MED 2018-042 du 30 octobre 2018 mettant en demeure la société X, available at: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037594451/, last accessed 23/03/2021].

These bid requests came from 32,708 different apps. Vectaury was a rather small company with an annual turnover of only 3.2 million (2017). OpenRTB makes this possible for hundreds or thousands of DSPs [cf. on the procedure in German *Herbrich*, DSB 2019, 34].

Each of these companies receives bid requests containing personal and also sensitive data of a large number of data subjects.



Graphic by Irish Council for Civil Liberties (ICCL)

No safeguards exist in the form of technical or organisational measures to ensure that a company, such as a DSP, that receives personal data in a bid request does not share it with other organizations (including so-called data brokers) or process it in a way or for a purpose that is not in accordance

with the data subjects' wishes. Defendant 1 stated in May 2018:

> *"[...] there is no technical way to limit the way data is used after the data is received by a vendor for decisioning/bidding on/after delivery of an ad [...]".*

In the same document, the 1st defendant pointed out the extremely high number of companies that can receive data and share or process it without permission:

> *"Surfacing thousands of vendors with broad rights to use data w/out tailoring those rights may be too many vendors/permissions [...]".*

Offer of Proof: Entire printout of the technical specification of defendant 1 and IAB Europe A.I.S.B.L. , Pubvendors.json v1.0: Transparency & Consent Framework, as amended May 2018, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md, last accessed 23/03/2021,

already submitted as **Annex K 12**

The UK's data protection regulator, the ICO, in its report on Real Time Bidding [Information Commissioner's Office, "Update report into adtech and real time bidding", 20.06.2019, available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, last accessed 10.02.2021, previously submitted as **Annex K 58**, p. 21 f.] 2019 notes:

> *"[...] there are no guarantees or technical controls about the processing of personal data by other parties, eg retention, security etc.. In essence, once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls".*

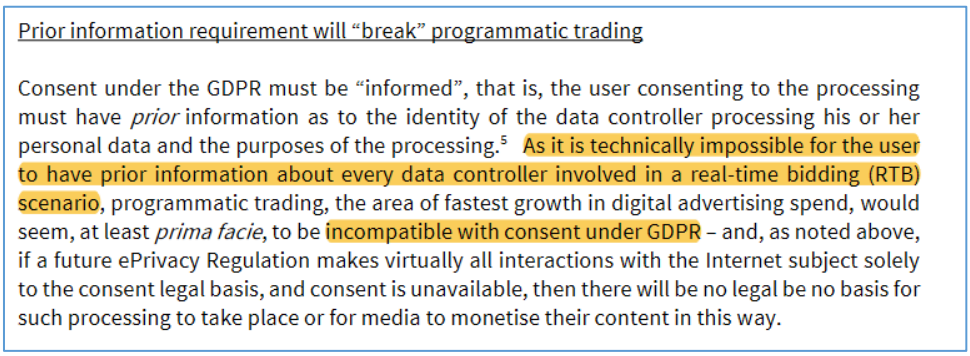
As a result, data subjects have no control over their data after a bid request has been sent. It is not possible for them to track who has received their data and how these entities process it, or to exercise their data subject rights under art. 15 et seq. GDPR.

The international weekly newspaper The *Economist* called the defendant 1's OpenRTB specifications a "[...] data protection-free zone [...]". The article [*The Economist*, 23 March 2019, p. 21] states with regard to defendant 1's OpenRTB standard:

> *"[...] builds in incentives to get as much data to as many bidders as feasible. And that is not particularly conducive to the protection of privacy. " [...]"*

For this reason, a year before defendant 1 and IAB Europe launched the "Transparency & Consent Framework", IAB Europe's Managing Director, A.I.S.B.L., Townsend Feehan, wrote to the EU Commission saying that an exception to the e-privacy regulation for OpenRTB needed to be created, otherwise online advertising could no longer be viable.

> *"[...] it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario [...]"*



Prior information requirement will "break" programmatic trading

Consent under the GDPR must be "informed", that is, the user consenting to the processing must have *prior* information as to the identity of the data controller processing his or her personal data and the purposes of the processing.[5] As it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario, programmatic trading, the area of fastest growth in digital advertising spend, would seem, at least *prima facie*, to be incompatible with consent under GDPR – and, as noted above, if a future ePrivacy Regulation makes virtually all interactions with the Internet subject solely to the consent legal basis, and consent is unavailable, then there will be no legal be no basis for such processing to take place or for media to monetise their content in this way.

Offer of Proof: Partial printout of letter from Townsend Feehan, CEO of IAB Europe A.I.S.B.L., June 26, 2017, available at: https://www.iccl.ie/wp-content/uploads/2020/10/IAB-to-Commission-email-and-attachment-26-June-2017.pdf (archived), accessed 03/24/2021,

presented as **Annex K 59**

Offer of Proof: Letter from Townsend Feehan, CEO of IAB Europe A.I.S.B.L., June 26, 2017, available at: https://www.iccl.ie/wp-content/uploads/2020/10/IAB-to-Commission-email-and-attachment-26-June-2017.pdf (archived), accessed 04/15/2021,

presented as **Annex K 60**

Every day, billions of personal and sensitive data are broadcast by OpenRTB. One advertising exchange called IndexExchange broadcasts 120 billion bid requests per day.

Offer of Proof: Entire printout from website indexexchange.com, *Meropol,* Meeting 2020's Business Challenges with Machine Learning, IX Traffic Filter, Aug. 06, 2020, available at: www.indexexchange.com/ix-traffic-filter-meeting-2020s-business-challenges-with-machine, last accessed Mar. 24, 2021,

submitted as **Annex K 61**

Pubmatic, also an advertising exchange that uses the 1st defendant's technical standard, sends 100 billion advertisements daily.

Offer of Proof: Entire printout from PubMatic's website, *Jain,* Optimizing data processing at scale, 10 Jun 2020, available at https://pubmatic.com/blog/optimizing-data-processing-at-scale, accessed on: 24.03.2021,

submitted as **Annex K 62**

Advertising Exchange OpenX says it receives 100 billion requests for ads every day, which indicates that it sends as many daily bid requests.

Offer of Proof: Printout from Google's website, OpenX: Power the future of advertising with Google Cloud, available at: https://cloud.google.com/customers/openx, last accessed 03/24/2021,

submitted as **Annex K 63**

These three Advertising Exchanges are estimated to have conducted 113.9 trillion OpenRTB auctions in 2020. There are other large Advertising Exchanges for which no information is available, including Google's Advertising Exchange, which also uses OpenRTB.

Offer of Proof: Entire printout from Google's website, OpenRTB Integration, available at: https://developers.google.com/authorized-buyers/rtb/openrtb-guide, last accessed 03/24/2021,

submitted as **Annex K 64**

Google's Advertising Exchange is used on 13.5 million websites [data from BuiltWith.com, available at: https://trends.builtwith.com/ads/DoubleClick.Net, last accessed 03/21/2021].

Google itself has not published figures on daily auction volumes, but an analysis by the UK Competition Authority shows that it is by far the largest advertising exchange [UK Competition & Markets Authority, Online platforms and digital advertising Market study final report, 01.07.2020, p. 20, available at: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, last accessed 23.03.2021]. The Authority concludes that it has market power in OpenRTB, which means that its dominance is such that it can charge higher prices.

Thus, it becomes clear that personal data is broadcast hundreds of billions of times a day through OpenRTB. Hundreds of trillions of bid requests are therefore processed annually by an unknown number of companies.

The provided security mechanisms of OpenRTB are not effective for the following reasons:

b) The IAB Transparency & Consent Framework

In April 2018, the 1st defendant, together with IAB Europe A.I.S.B.L., announced that a security mechanism would be introduced for the OpenRTB system: the Transparency & Consent Framework ("TCF"). They claimed that the TCF would give data subjects full control over their data. This is not the case.

The TCF is another standard. The TCF defines how information on the existence and scope of the data subject's consent to the processing of personal data in OpenRTB auctions is communicated between actors. Signals stating that the data received may not be processed further are provided for. However, the system has no means of actually controlling or limiting access.

Whether or not a company uses TCF does not in any respect affect what processing it actually does with the data it receives via OpenRTB bid requests. For example, there are no measures in place to prevent a company that receives OpenRTB data from copying and transmitting it to others, or from using it for any other conceivable purposes. Nor is there any way to verify that the TCF signal has been honored or ignored.

Item 6.5 of the TCF policy states:

> "*[...] If a CMP has reasonably believes that a Vendor is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Europe according to MO procedures and may, as provided for by MO procedures, pause working with the Vendor while the matter is addressed. . [...]".*

Offer of proof: Full printout from IAB Europe A.I.S.B.L. website. , IAB Europe Transparency & Consent Framework Policies, version 2020-08-24.3.2, 2019, p. 11, available at: https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf, last accessed on 24/03/2021,

presented as **Annex K 65**

It is clear from the word "may" that if a company has reasonable grounds to believe that a vendor is not behaving in accordance with the rules, it is merely permitted to cease cooperation with him. There is no obligation to discontinue.

It is a self-regulatory mechanism based on the assumption that the participating companies comply with it voluntarily.

The General Terms and Conditions of the TCF do not provide any protection either. IAB Europe A.I.S.B.L. stated in response to a request (Challenge) from the Belgian data protection authorities [Letter from IAB Europe A.I.S.B.L. to Belgian Data Protection Commission, 10.02.2020, p. 10]:

> *"[...] The Terms and Conditions themselves are not intended to protect personal data or to impose obligations under the GDPR. We therefore do not know how and why the Terms and Conditions could (or should) take into account the GDPR and its referenced provisions. It is the TCF that serves as a tool for companies to comply with certain aspects of the GDPR, not the Terms and Conditions" [...].*

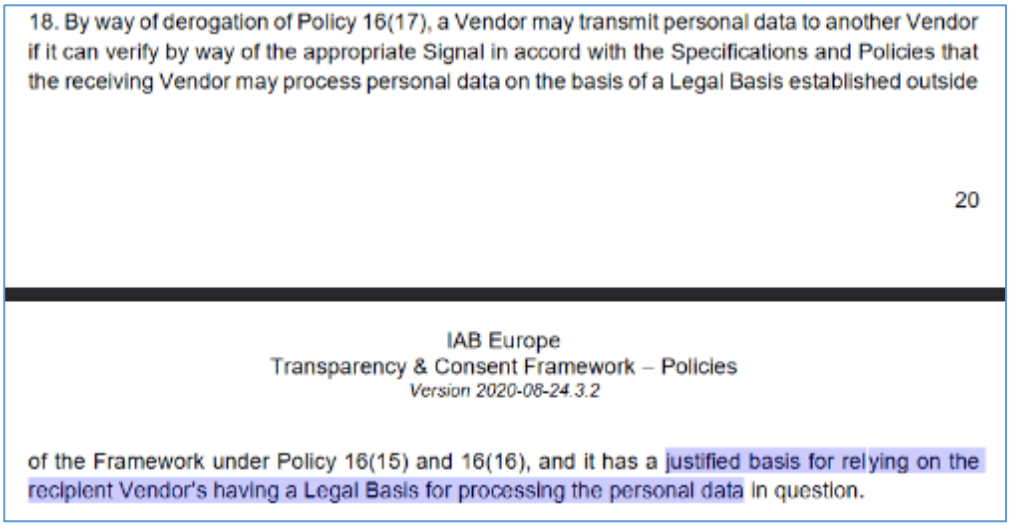
Nor is there any way to verify or audit what companies that have received IAB OpenRTB data have done with it. The TCF Policy does not define any way in which the 1st defendant or any other

organization could conduct any verification in this regard. Given the scale of the data processing and transfers, it is not possible to do so.

The TCF therefore cannot guarantee the protection of personal data; nor the lawfulness or the transparency of the processing. Nor can changes to the TCF create mechanisms that do so, because no one can control what happens to personal data after they have been broadcast in a bid request.

Another problem with the TCF is that it anticipates that recipients of bid requests will share them with third parties, regardless of whether there is a legal basis for doing so or whether there are adequate safeguards to ensure data security. The TCF states that any company is free to share data with others because it is based on a

"[...] justified basis for relying on the recipient vendor's having a legal basis for processing personal data [...]".


18. By way of derogation of Policy 16(17), a Vendor may transmit personal data to another Vendor if it can verify by way of the appropriate Signal in accord with the Specifications and Policies that the receiving Vendor may process personal data on the basis of a Legal Basis established outside

20

IAB Europe
Transparency & Consent Framework – Policies
Version 2020-08-24.3.2

of the Framework under Policy 16(15) and 16(16), and it has a justified basis for relying on the recipient Vendor's having a Legal Basis for processing the personal data in question.

Offer of Proof: Partial printout from IAB Europe A.I.S.B.L. website. , IAB Europe Transparency & Consent Framework Policies, version 2020-08-24.3.2, 2019, p. 21, available at: https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf, accessed 23/03/2021,

submitted as **Annex K 66**

Thus, TCF grants companies absolute freedom to process and disseminate personal data even if they know that a recipient is in breach of data protection law. The mechanism relies on trust in the

good will of hundreds of companies whose business model is to trade in personal data.

As shown in detail under A. IV. 2. c) p. 117, the TCF signals themselves are in turn used to broadcast recordings of the website visits and app uses of the data subjects. Perfidiously, the alleged protection mechanism is thus yet another tracking method.

c) The assumption of general compliance

OpenRTB is a system that disseminates personal and sensitive data on a large scale. The Transparency & Consent Framework of IAB Europe, A.I.S.B.L., offers no protection to data subjects. The only remaining safeguard is an accumulation of statements in the technical protocols of the 1st defendant, according to which the participating companies are expected to ensure the conformity of their actions with all applicable legal standards.

Elsewhere, the 1st defendant states:

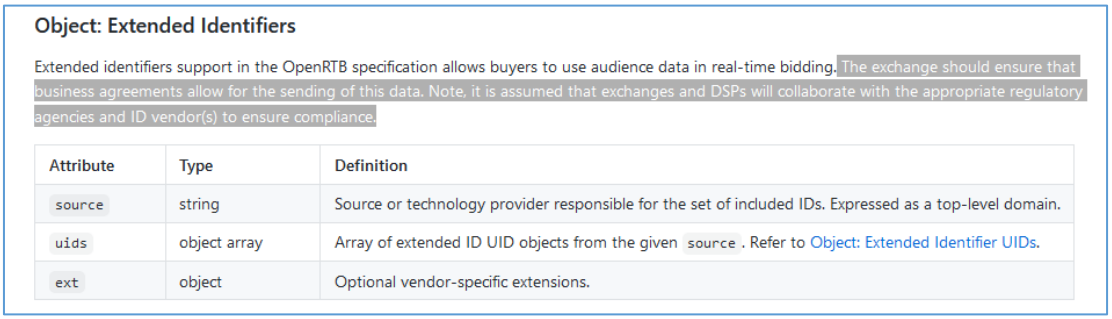
> "*[...] all exchanges that use the protocol - which together constitute the vast majority of activity in the programmatic ecosystem - should account for all local legislation and not pass any content taxonomy node that is flagged as "sensitive data". This guidance was also applied to specific sections of the protocol, including the Ad Object, Content Object, Publisher Object, User Object, and Data Object. Together with the additional sensitive data signals contained within the Content Taxonomy, downstream platforms should now have much more context to inform data storage and segmentation practices. [...]"*

Offer of Proof: Entire Printout of 1st defendant's Public Statement, Tech Lab Introduces Additional Consumer Privacy Safeguards into Content and Audience Taxonomies, Apr. 30, 2020, available at: https://iabtechlab.com/blog/tech-lab-introduces-additional-consumer-privacy-safeguards-into-content-and-audience-taxonomies/, last accessed Mar. 24, 2021,

submitted as **Annex K 67**

On the use of "Extended Identifiers" it states:

> *"[...] the exchange should ensure that business agreements allow for the sending of this data. Note, it is assumed that exchanges and DSPs will collaborate with the appropriate regulatory agencies and ID vendor(s) to ensure compliance. [...]"*



Object: Extended Identifiers

Extended identifiers support in the OpenRTB specification allows buyers to use audience data in real-time bidding. The exchange should ensure that business agreements allow for the sending of this data. Note, it is assumed that exchanges and DSPs will collaborate with the appropriate regulatory agencies and ID vendor(s) to ensure compliance.

Attribute	Type	Definition
`source`	string	Source or technology provider responsible for the set of included IDs. Expressed as a top-level domain.
`uids`	object array	Array of extended ID UID objects from the given `source`. Refer to Object: Extended Identifier UIDs.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of the technical specifications of the Protocol of 1st defendant, IABTechLab, Inc., AdCOM Specifications v1.0, June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_eids, last accessed 03/24/2021,

presented as **Annex K 68**

The 1st defendant thus expects thousands of companies participating in OpenRTB to protect personal data, including special category data. It has not itself taken any measures to ensure security. Relying on such a large number of companies to behave righteously does not constitute a security measure.

5. Responsibilities of the defendants

The contributions of the individual defendants to the data processing at issue are set out below.

(a) contributions by the 1st defendant

The 1st defendant developed the global standards that determine Real Time Bidding worldwide and thereby created the necessary precondition for the processing operations at issue. It organizes, coordinates and facilitates the data processing operations that take place. Moreover, it encourages them.

(aa) organisation of data processing

The 1st defendant organizes the processing of the plaintiff's personal and sensitive data in dispute when websites and apps are called up (see point A. II. 3., p. 28 f.) by providing website operators

(publishers) and SSPs and DSPs as well as DMPs with the technical standards OpenRTB, AdCOM, Content Taxonomy, and Audience Taxonomy. They form the framework for the global functioning of the targeting of personalized advertising in RTB auctions of online advertising space on websites and in apps. The standards are a prerequisite for the successful interaction of the players. The defendant 1's protocol OpenRTB was created to standardize RTB broadcasts of personal data in the online advertising industry.

> *"[...] The mission of the IAB OpenRTB project is to spur growth in Real-Time Bidding (RTB) marketplaces by providing open industry standards for communication between buyers of advertising and sellers of publisher inventory. [...]"*

Offer of Proof: IAB TechLab, OpenRTB API Specification Version 2.5, December 2016, Document 44, available at https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf, accessed 23/03/2021, p. 2,

already submitted as **Annex K 46**

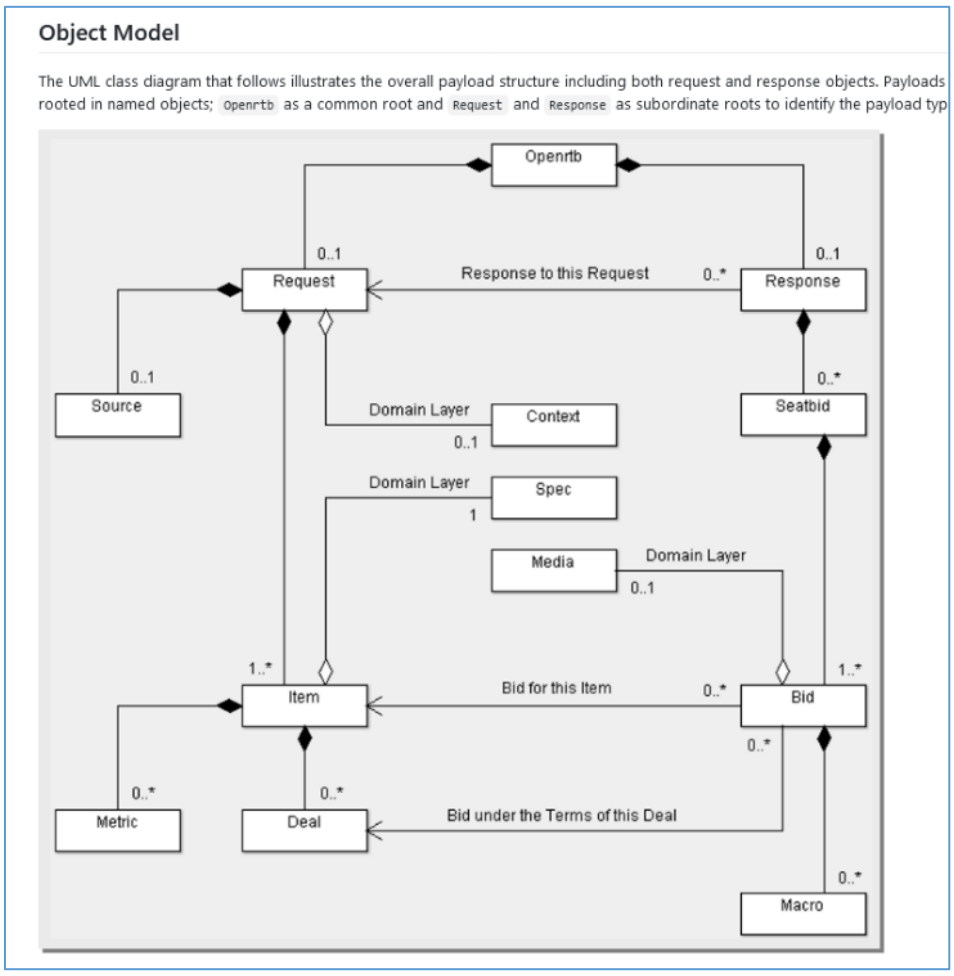
bb) Coordination of data processing

The 1st defendant has developed and published the technical standards OpenRTB, AdCOM, Content Taxonomy and Audience Taxonomy. It defines which personal data can be transmitted in bidding requests and determines the rules according to which auctions for online advertising spaces are conducted and advertisements are delivered. This concerns, for example, the rules for the sharing exchange of the plaintiff's personal data in a bid request when a publisher's website is loaded, and the corresponding response by the third-party platforms involved.

Defendant 1's OpenRTB Specifications v3.0 protocol states [see entire printout of defendant 1's protocol technical specifications, OpenRTB Specification 3.0, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md, already submitted as **Annex K 16**]:

> *"The overall goal of IAB OpenRTB is and has been to create a lingua franca for communicating between buyers and sellers. "*

As this states, the 1st defendant sets the rules and basic structure for the exchange of bid requests and bid responses, as well as for the conclusion of an auction:



Offer of Proof: Partial Printout of 1st defendant's Protocol Technical Specifications, OpenRTB Specification v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#objectmodel, last accessed 03/24/2021,

presented as **Annex K 69**

Companies must abide by these rules, and submit to corresponding contractual obligations vis-à-vis the 1st defendant in order to be able to use the 1st defendant's technical specifications.

Offer of Proof: Entire printout of 1st defendant's website, Terms of Use, as amended Dec. 10, 2014, available at: https://iabtechlab.com/terms-of-use/, last accessed Mar. 24, 2021,

submitted as **Annex K 70**

The OpenRTB standard and associated documents recommend the use of unique identifiers for users of websites. They provide for the broadcast of information about their online user behaviour, and the classification of their interests.

In addition, representatives of defendant 1 emphasize the need for unique identifiers for website users in public statements. For example, a senior executive of defendant 1 told industry representatives that identifiers are essential:

> *"[...] brand agency use cases rely on identifiers: audience targeting, basic measurement functions like reach and frequency capping, and just being able to count impressions and clicks.... All these use cases are at risk as identifiers are removed [...]".*

Evidence quote: Video recording: How the removal of identifiers impacts agencies and advertisers, IAB TechLab event of 21.07.2020, available at: https://vimeo.com/442504076

Another representative of the 1st defendant reiterated that:

> "[...] identifiers and addressability fuel all core ad-supported use cases and systems [...]".

Evidence quote: Video recording: Jordan Mitchell, IAB TechLab presentation, Identity, Project Rearc, Privacy Sandbox - Webinar, IAB TechLab, 04.06.2020 available at: https://youtu.be/Z4VUOrUNETI, last accessed 26.11.2020

cc) Encouraging data processing

In addition to the development of these standards and protocols, the 1st defendant also supports

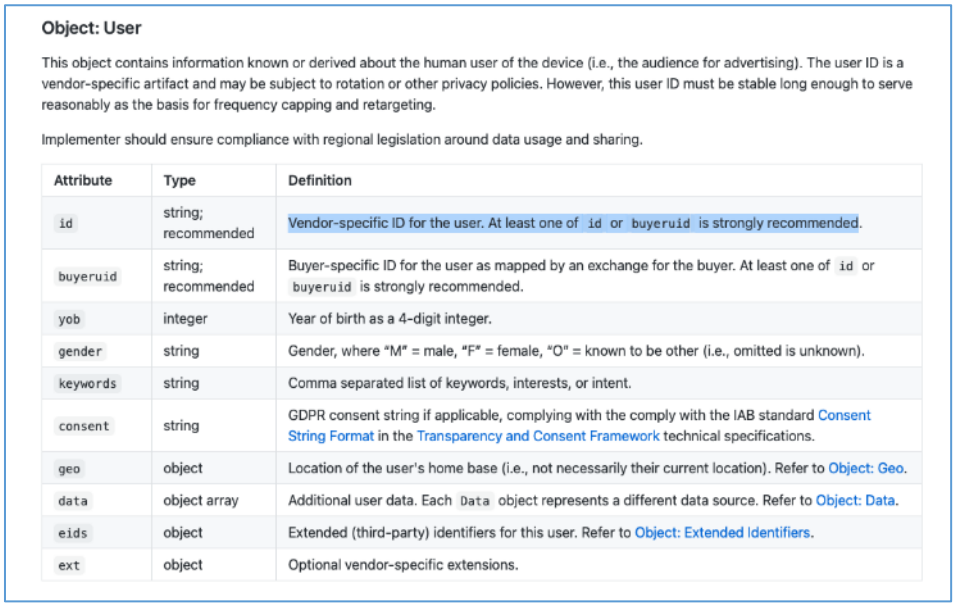
publishers, providers of SSPs and DSPs as well as online advertising exchanges in the implementation i.e. integration, of the technical standards OpenRTB, AdCOM, Content Taxonomy, and Audience Taxonomy [see defendant's press release dated 09.06.2020, available at: https://iabtechlab.com/press-releases/tech-lab-increases-investment-presence-in-europe/, already submitted as **Annex K 5**]. Thereby, the 1st defendant enables and encourages the processing of personal and sensitive data of the Plaintiff when loading the 3rd defendant's website (cf. pt. A. II. 3, p. 28).

In addition, defendant 1 encourages its members to process personal data by providing assistance in implementing its protocols, and through training programs that promote data sharing specified in the OpenRTB, AdCOM, Content Taxonomy, and Audience Taxonomy technical standards. For example, an employee of defendant 1 stated in a webinar on personal identifiers that the removal of users' identifiers (personal data such as Plaintiff's IP address and User ID) would underlie various advertising agency services:

> *"[...] brand agency use cases rely on identifiers: audience targeting, basic measurement functions like reach and frequency capping, and just being able to count impressions and clicks. [...] All these use cases are at risk as identifiers are removed [...]."*

Offer of Proof: Video recording: 'How the removal of identifiers impacts agencies and advertisers', dated 21/07/2020, available at: https://vimeo.com/442504076, last accessed 10/02/2021.

The use of personal identification codes about people who visit websites in bid requests is even "strongly recommended" in the technical standard AdCOM Specifications v1.0, and thus made a essential for the normal functioning of the standard:



Object: User

This object contains information known or derived about the human user of the device (i.e., the audience for advertising). The user ID is a vendor-specific artifact and may be subject to rotation or other privacy policies. However, this user ID must be stable long enough to serve reasonably as the basis for frequency capping and retargeting.

Implementer should ensure compliance with regional legislation around data usage and sharing.

Attribute	Type	Definition
`id`	string; recommended	Vendor-specific ID for the user. At least one of `id` or `buyeruid` is strongly recommended.
`buyeruid`	string; recommended	Buyer-specific ID for the user as mapped by an exchange for the buyer. At least one of `id` or `buyeruid` is strongly recommended.
`yob`	integer	Year of birth as a 4-digit integer.
`gender`	string	Gender, where "M" = male, "F" = female, "O" = known to be other (i.e., omitted is unknown).
`keywords`	string	Comma separated list of keywords, interests, or intent.
`consent`	string	GDPR consent string if applicable, complying with the comply with the IAB standard Consent String Format in the Transparency and Consent Framework technical specifications.
`geo`	object	Location of the user's home base (i.e., not necessarily their current location). Refer to Object: Geo.
`data`	object array	Additional user data. Each `Data` object represents a different data source. Refer to Object: Data.
`eids`	object	Extended (third-party) identifiers for this user. Refer to Object: Extended Identifiers.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of defendant 1's Protocol Technical Specifications, AdCOM Specifications v1.0, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_user,

already submitted as **Annex K 20**

dd) Facilitation of data processing

Irrespective of the fact that the 1st defendant already supports the processing of the plaintiff's personal data by providing the technical standards and by laying down rules (see A. II. 3., p. 28), the 1st defendant also facilitates the data processing in question.

It has developed a tool called "OpenRTB Validator", which allows companies to check whether they have properly inserted personal data in their bid requests and accompanying data transfers. The OpenRTB Validator tool is available at: https://ortbvalidator.iabtechlab.com/login (last accessed 24/03/2021) and is a significant contribution to facilitating data processing in accordance with the standards defined by the 1st defendant.

Offer of Proof: Partial printout of defendant's website as of 3/24/2021, available at: https://ortbvalidator.iabtechlab.com/login, last accessed 3/24/2021,

submitted as **Annex K 71**

It also provides a document to facilitate the trade of personal data between data broker companies and advertising technology companies. This is a form in which core information about data sets available for sale. The information includes the origin of the data, the audience taxonomy segments to which the data subjects have been classified, and the countries from which the data sets originate.

Offer of Proof: Entire printout of defendant 1's website, Data Transparency Standard 1.0, as amended 6/27/2019, available at: https://iabtechlab.com/wp-content/uploads/2019/06/Data-Transparency-Standard-1.0-Final-June-2019.pdf, last accessed 3/24/2021,

as **Annex K 72**

(b) contributions by the 2nd defendant

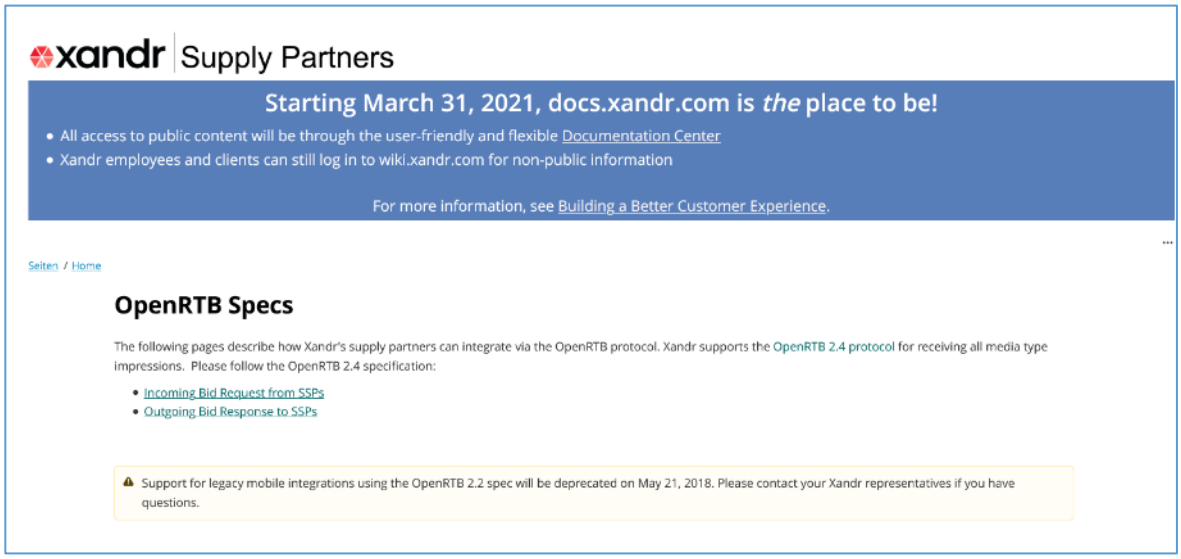
Defendant 2 operates a platform that allows the buying and selling of inventory from multiple advertising exchanges [see Wikipedia: Ad Exchange, available at: https://en.wikipedia.org/wiki/Ad_exchange, accessed on 22.03.2021].

Offer of Proof: Partial printout of Adzine.com website, Xander - Infrastructure for the Global Advertising Ecosystem, as amended 3/24/2021, available at: https://www.adzine.de/techfinder/xandr/, accessed 3/24/2021,

submitted as **Annex K 73**

This platform receives OpenRTB bid requests from SSPs and forwards them to DSPs. Defendant 2 uses defendant 1's standards for this purpose, namely:

OpenRTB 2.4, i.e. the previous version of the current standard of the 1st defendant.



Offer of Proof: Partial printout of 2nd defendant's website, Documentation Center: OpenRTB Specs, as amended 03/22/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/openrtb-specs.html, last accessed 02/22/2021,

submitted as **Annex K 74**

The contribution of the 2nd defendant to the data processing in dispute (cf. already point A. II. 3., p. 27f.) is not only the mere provision of a platform as a central infrastructure where website operators such as the 3rd defendant can view guidelines for the integration of Real Time Bidding - based on the technical standards of the 1st defendant - and download programming codes for the implementation of the real-time auction of advertising spaces.

Rather, defendant 2 provides website operators such as defendant 3 with detailed specifications for integrating the programming code for conducting the real-time auction of advertising space based on defendant 1's technical standards.

Offer of Proof: Partial printout of 2nd defendant's website, OpenRTB Integration Process, as of 03/29/2021 available at: https://docs.xandr.com/bundle/supply-partners/page/faq---integration-process.html, last accessed 03/29/2021,

submitted as **Annex K 75**

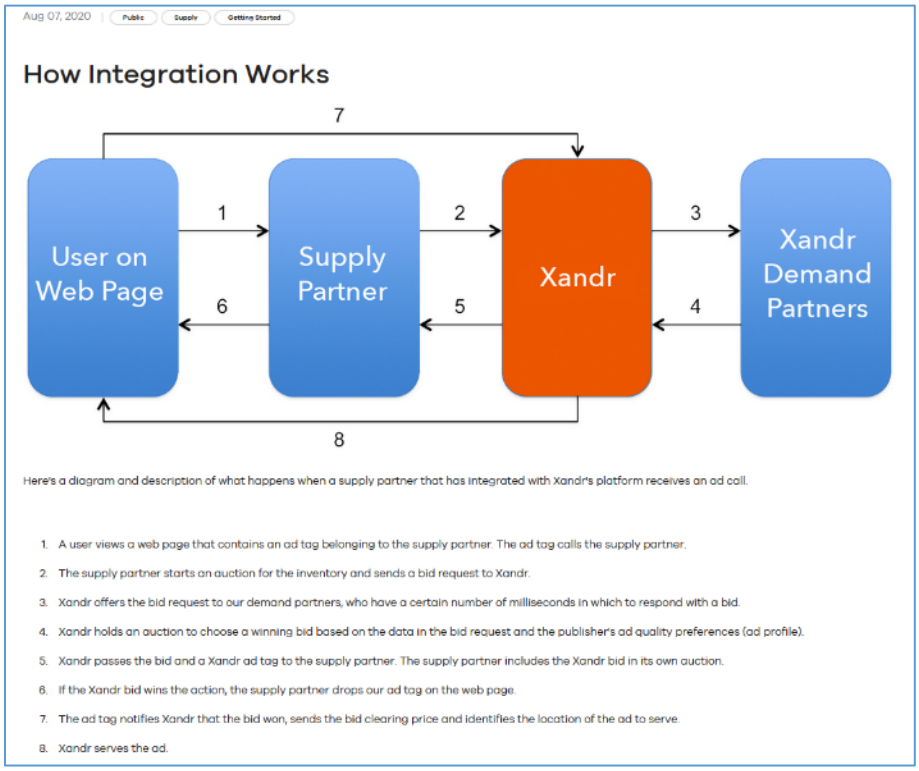
In addition, defendant 2 explicitly provides program code (API integration and JSON Fields) to publishers such as defendant 3.

Offer of Proof: Partial printout of 2nd defendant's website, Documentation Center: Publisher Services, as amended 01.04.2021 available at: https://docs.xandr.com/bundle/xandr-api/page/publisher-service.html, last accessed 01.04.2021,

submitted as **Annex K 76**

Specifically, in its "Documentation Center," defendant 2 describes its participation in the real-time auction of advertising space in eight steps as follows:

- A user loads a website/app such as that of the 3rd defendant, which contains an "ad tag" (code) belonging to the "supply partner". The ad tag calls the supply partner.
- The supply partner starts an auction for the inventory and sends a bid request to defendant 2.
- Defendant 2 offers the bid request to "demand partners", who have a certain number of milliseconds to respond with a bid.
- Defendant 2 holds an auction to select a winning bid based on the data in the bid request and the defendant 3's (the publisher) ad quality preferences (ad profile).
- Defendant 2 passes the bid and its "ad tag" to the supply partner. The sales partner includes the bid in its own auction.
- If defendant 2's bid wins, the supply partner places defendant 2's ad tag on defendant 3's website, for example.
- The ad tag notifies the 2nd defendant that the bid won, sends the bid clearing price, and identifies the location of the ad to be placed.
- Defendant 2 places the advertisement on defendant 3's website.



Aug 07, 2020 | Public | Supply | Getting Started

How Integration Works

Here's a diagram and description of what happens when a supply partner that has integrated with Xandr's platform receives an ad call.

1. A user views a web page that contains an ad tag belonging to the supply partner. The ad tag calls the supply partner.
2. The supply partner starts an auction for the inventory and sends a bid request to Xandr.
3. Xandr offers the bid request to our demand partners, who have a certain number of milliseconds in which to respond with a bid.
4. Xandr holds an auction to choose a winning bid based on the data in the bid request and the publisher's ad quality preferences (ad profile).
5. Xandr passes the bid and a Xandr ad tag to the supply partner. The supply partner includes the Xandr bid in its own auction.
6. If the Xandr bid wins the action, the supply partner drops our ad tag on the web page.
7. The ad tag notifies Xandr that the bid won, sends the bid clearing price and identifies the location of the ad to serve.
8. Xandr serves the ad.

Offer of Proof: Partial printout of 2nd defendant's website, Documentation Center: How Integration Works, as amended 03/25/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/how-integration-works.html, last accessed 03/25/2021,

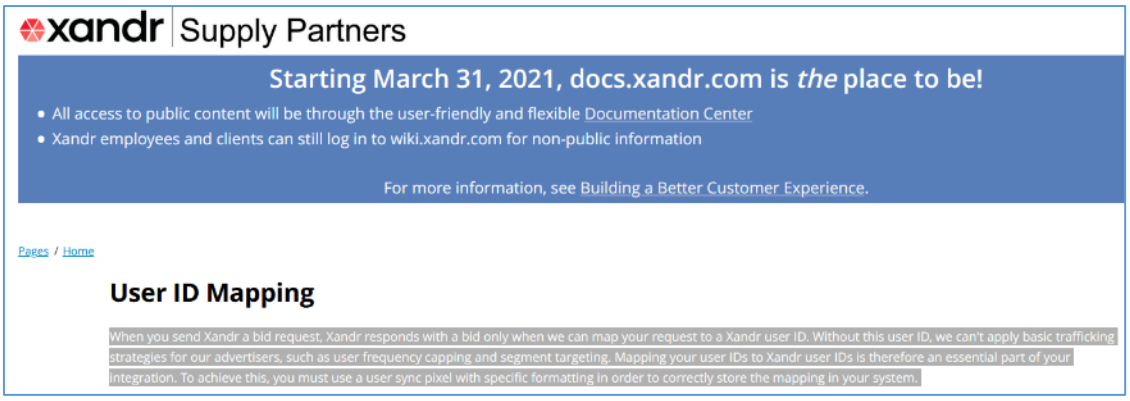
submitted as **Annex K 77**

The 2nd defendant admits that it only accepts bid requests from SSPs if a "Xandr user ID" is included, in order to enable "segment targeting", i.e. the use of categories from the 1st defendant's technical standard (cf. already point A. II. 2. d. , p. 28) for the placement of advertisements.

Defendant 2 says that matching the "Xandr user IDs" with user IDs (e.g. cookie IDs) of SSPs and website operators such as the 3rd defendant is also necessary in the run-up to a real-time auction in order to be able to practice real-time bidding.

> *"When you send Xandr a bid request, Xandr responds with a bid only when we can map your request to a Xandr user ID. Without this user ID, we can't apply basic trafficking strategies for our advertisers, such as user frequency capping and segment targeting. Mapping your user IDs to Xandr user IDs is therefore an essential part of your*

integration. To achieve this, you must use a user sync pixel with specific formatting in order to correctly store the mapping in your system. […]"



Offer of Proof: Partial printout of 2nd defendant's website, Documentation Center: User ID Mapping, as amended 03/25/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/user-id-mapping.html, last accessed 03/25/2021,

presented as **Annex K 78**

Finally, the 2nd defendant is a member of the 1st defendant and in this way contributes to the development and provision of the technical standards [see partial printout of the 1st defendant's website dated 23/03/2021 on IAB Tech Lab Members, available at: https://iabtechlab.com/about-the-iab-tech-lab/iab-tech-lab-members/, last accessed 23/03/2021, already submitted as **Annex K 4**].

(c) contributions by the 3rd defendant

The 3rd defendant operates the website at the URL https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten.

As shown in section A. II. 3., p. 27, the 3rd defendant has actively implemented programming codes of the 2nd defendant in the source code of its website, which were developed on the basis of the 1st defendant's technical standards. Due to the integration of the programming codes of the 2nd defendant, several server requests for the execution of Real Time Bidding auctions are triggered to the 2nd defendant as well as to other advertising exchanges when the 3rd defendant's website is called up.

The 3rd defendant transmitted by server request the user ID ("uuid2"), cookie information and information on the plaintiff's browser settings, among other things, to the 2nd defendant. In the context of the server responses of the 2nd defendant about the results of the auction according to the technical standard "OpenRTB API Specifications Version 2.4" of the 1st defendant, the corresponding advertising material was played on the 3rd defendant's website.

The 3rd defendant integrated a tracking code of the 2nd defendant in the source code of the website "onlinemarketing.de", which enables the setting of a cookie of the 3rd defendant in the plaintiff's browser to conduct "User Mapping" with the 2nd defendant. The 2nd defendant has stated that this is absolutely necessary in the run-up to the real-time auction on the 3rd defendant's website [cf. partial printout of the 2nd defendant's website, Documentation Center: User ID Mapping, as amended on 25.03.2021, available at: https://docs.xandr.com/bundle/supply-partners/page/user-id-mapping.html, last accessed on 25.03.2021, already submitted as **Annex K 78**].

Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) with defendant 2,

already submitted as **Annex K 27**

III. Concerning motion 2

1. Information provided

The privacy notices on the website https://onlinemarketing.de do not contain any references to processing by the 2nd defendant or processing based on the 1st defendant's technical standards at issue.)

Offer of Proof: Entire printout of defendant 3's website privacy information, dated 03/22/2021, available at https://onlinemarketing.de/datenschutzerklaerungen, last accessed 03/22/2021,

already submitted as **Annex K 2**

Information on the essence of a joint responsibility agreement for the processing at issue within the meaning of the second sentence of art. 26 para. 2 of the GDPR is not provided in the 3rd defendant's "Privacy Statement" (**Annex 75)** nor in the "Privacy Information" (see **Annex 94).**

The defendants have failed to provide information on the substance of the agreement within the meaning of art. 26 para. 2 sentence 2 of the GDPR, despite entering into a joint responsibility agreement for the processing at issue pursuant to art. 26 para. 1 sentence 2 of the GDPR. The joint responsibility agreement between the defendants is in the exclusive domain of the defendants.

Offer of Proof: Motion for production of contract customer on joint responsibility by defendants.

2. Contributions by the defendants

With regard to the contributions of the defendant, reference is made to the motion to 1 (point A. II. 5., p. 80f.).

IV. Concerning motion 3

Within the scope of the processing processes at issue, which are based on the technical standards of the 1st defendant, OpenRTB, AdCOM, Content Taxonomy, and Audience Taxonomy, particularly sensitive data are also processed.

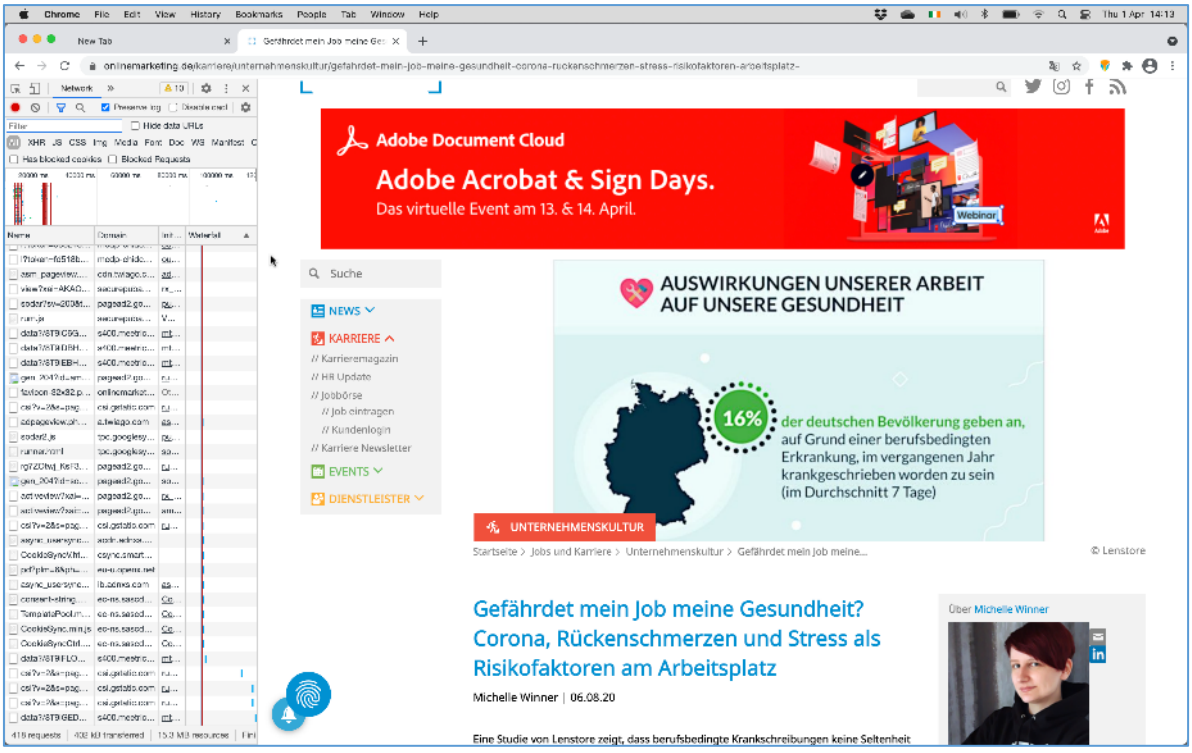
Article 9 para. 1 GDPR prohibits the processing of special categories of data unless specific conditions are met:

> "*[...] Processing of 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 shall be prohibited [...].*"

1. **Processing of particularly sensitive data triggered by visit to defendant 3's website: "Does my job put my health at risk?"**

The plaintiff accessed the website at the URL https://onlinemarketing.de/karriere/unternehmenskultur/gefahrdet-mein-job-meine-gesundheit-corona-ruckenschmerzen-stress-risikofaktoren-arbeitsplatz on 01.04.2021. There, an article with the title "Does my job endanger my health - Corona, back pain and stress as risk factors at work" is available.

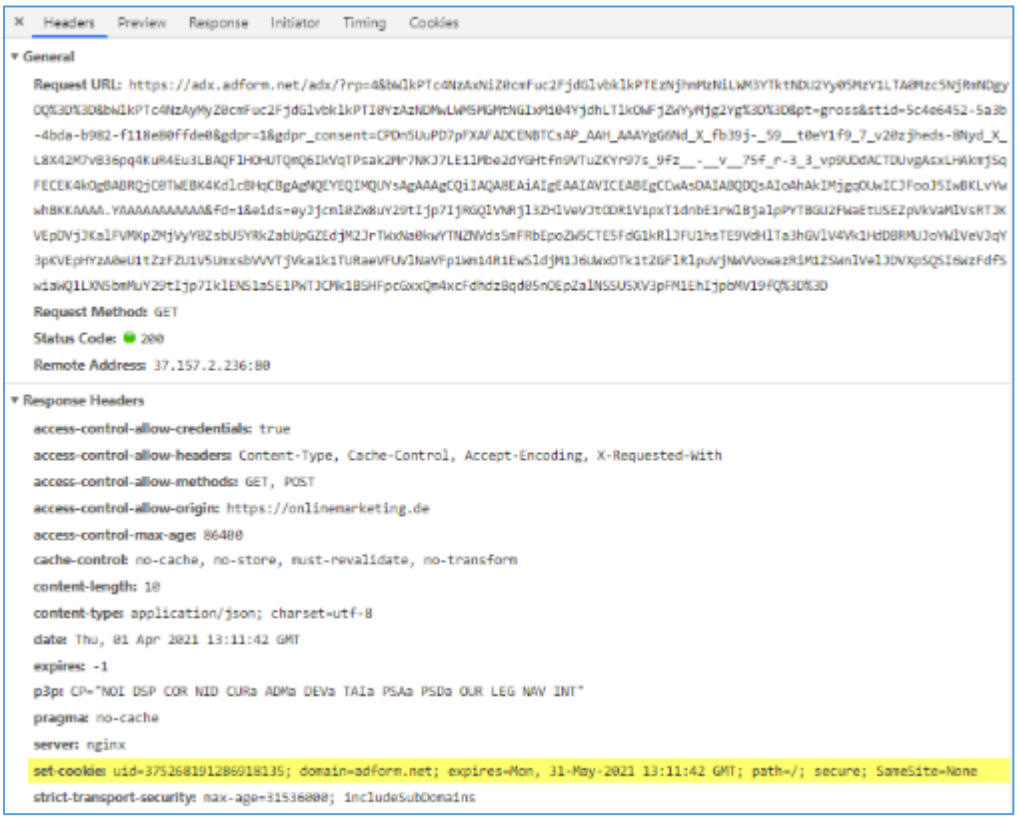
The same processing operations with regard to the personal data of the applicant took place as those already described under A. II. 3. (p. 27f.).



Offer of proof: Printout of the website of the defendant 3 under the URL: https://onlinemarketing.de/karriere/unternehmenskultur/gefahrdet-mein-job-meine-gesundheit-corona-ruckenschmerzen-stress-risikofaktoren-arbeitsplatz under display of the console for web developers of the standard browser Chrome from 01.04.2021,

submitted as **Annex K 79**

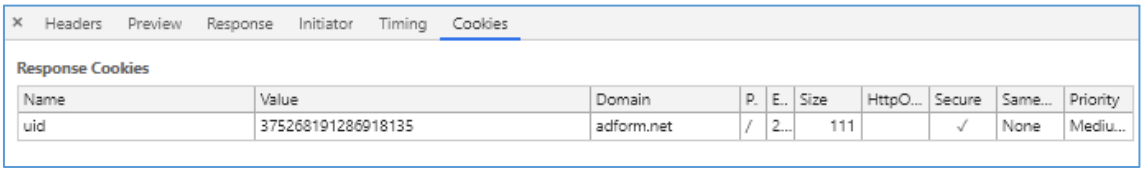
(1) When the plaintiff called up the website on 01.04.2021 at 2:11 p.m. (GMT+1 after time change, corresponds to 3:11 p.m. German time), a server request was sent from the plaintiff's browser ("Request URL") to Adform (https://adx.adform.net) with the request to set a cookie and to assign a user ID in the browser of the plaintiff's end device ("setcookie") due to the source code of the 3rd defendant. As part of the corresponding server response ("Response Headers"), Adform assigned plaintiff a User ID with the value (uid=375268191286918135), which was stored in the plaintiff's browser in Adform's cookie named "uid."



Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 04/01/2021 showing network connections (server request) using Adform,

submitted as **Annex K 80**

As a result of Adform's server response, the user ID (uid=375268191286918135) assigned by Adform was stored in Adform's cookie (uid) in the plaintiff's browser.



Offer of Proof: Partial printout of the website archive file (HAR file) of defendant 3's website dated 04/01/2021 showing network connections (server request) with Adform and plaintiff's browser web storage,

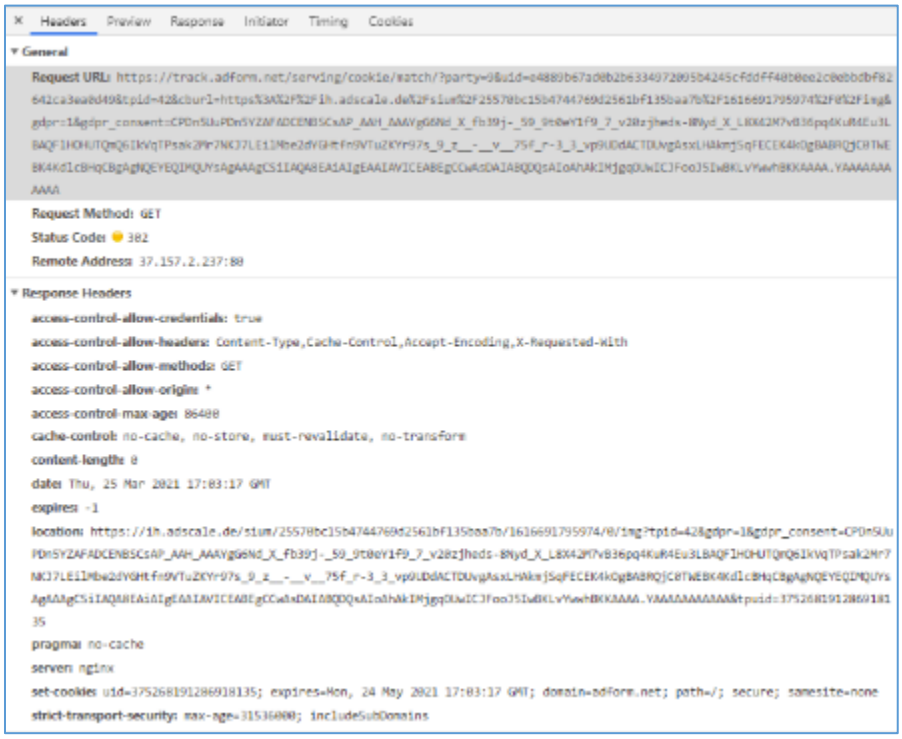
submitted as **Annex K 81**

(2) Adform operates a data marketplace. The personal data distributed there are classified into categories corresponding to those of the Audience Taxonomy of the 1st defendant.

Offer of Proof: Video Recording, Adform: Introducing Audience Marketplace for the Adform DSP, available at: https://vimeo.com/312698522, last accessed 03/24/2021,

Accordingly, sensitive information in the health context about the plaintiff's website visit was processed using the technical standard Audience Taxonomy of the 1st defendant. The same applies to the technical standard Content Taxonomy of the 1st defendant (cf. on this already point A. II. 3. a), p. 44).

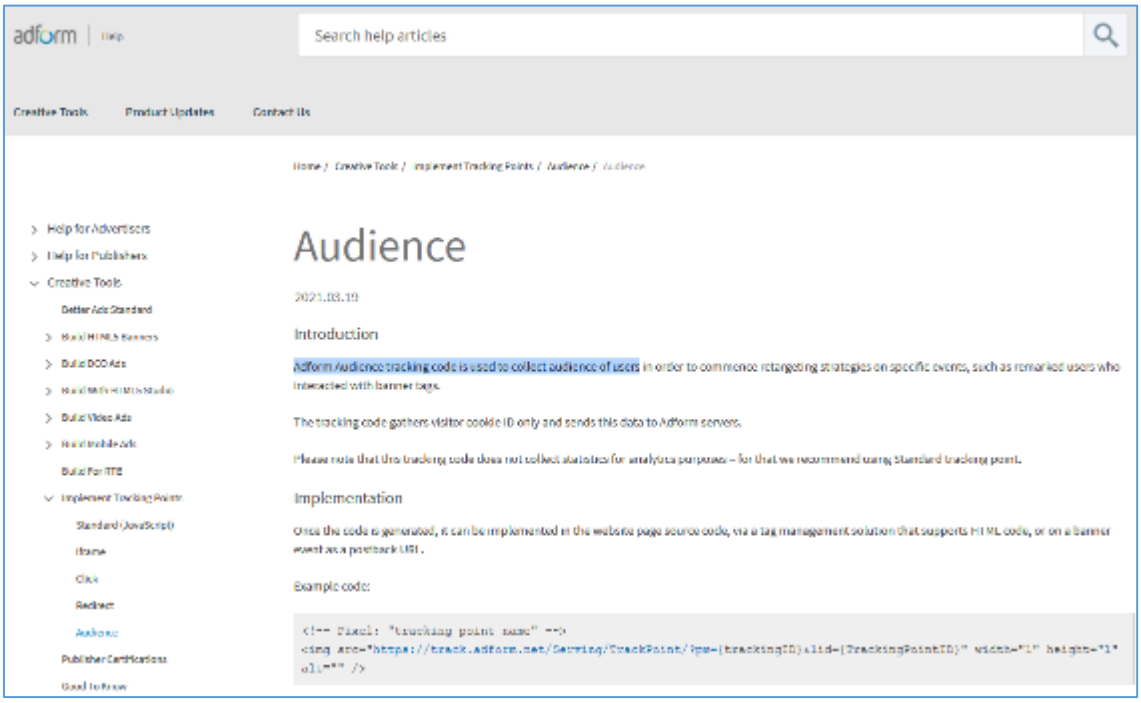
(3) When the plaintiff visited the website onlinemarketing.de, a server request (track.adform.net) was also sent to the company Adform Advertising, LLC. (1400 Parker Rd Baltimore, MD 21227, USA) to carry out the matching with other buying and SSPs for the execution of a Real Time Bidding auction.



Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 03/25/2021 showing network connections (server request) using Adform,

submitted as **Annex K 82**

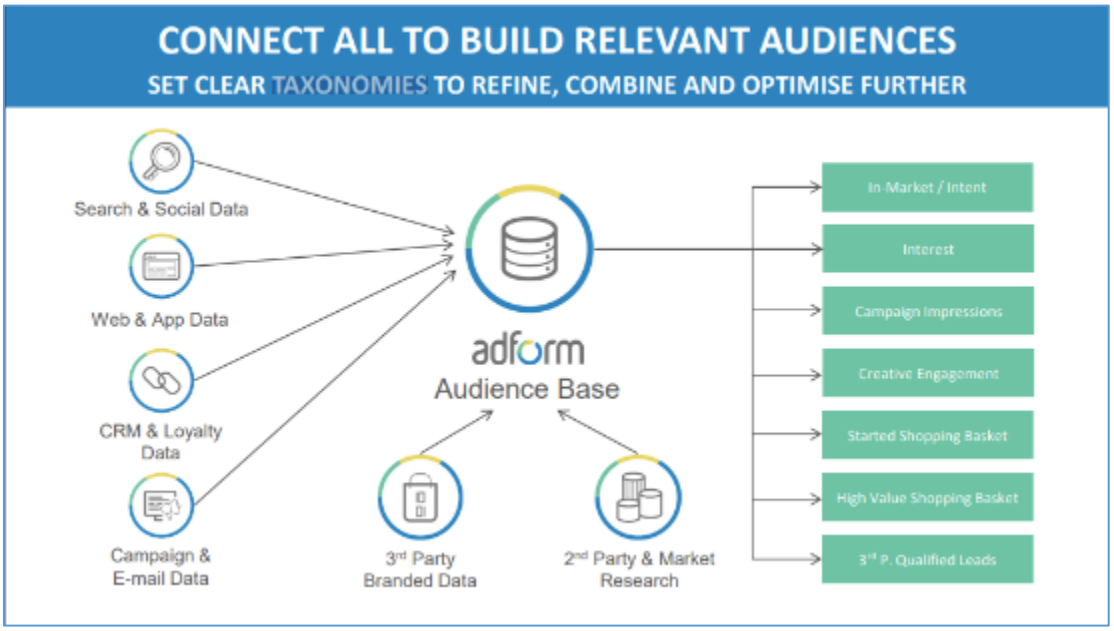
According to Adform's own statements, this "Adform Audience Tracking Code" (i.e. the above server request) is used to classify the plaintiff or the content he has accessed into categories defined by the technical standards Audience Taxonomy and Content Taxonomy of the 1st defendant. These categories disclose sensitive information about the plaintiff. The classification is used for the automated targeting of advertising.



Offer of Proof: Partial Printout of Adform's Integration Guide for Incorporating Tracking Code to Create Categories for Website Operators, as amended 03/19/2019, available at: https://www.adformhelp.com/s/article/UUID-7539fb22-b0ff-e321-b3f3-72e007106d9a, last accessed 04/06/2021,

submitted as **Annex K 83**

According to the plaintiff's own statements, the categorization of the plaintiff's personal data for sale on Adform's marketplace is also based on results from Internet search engines and social media, historical purchase data from advertisers' customer databases, e-mail addresses, and information from other data sources, such as arbitrary third parties and market research institutes.

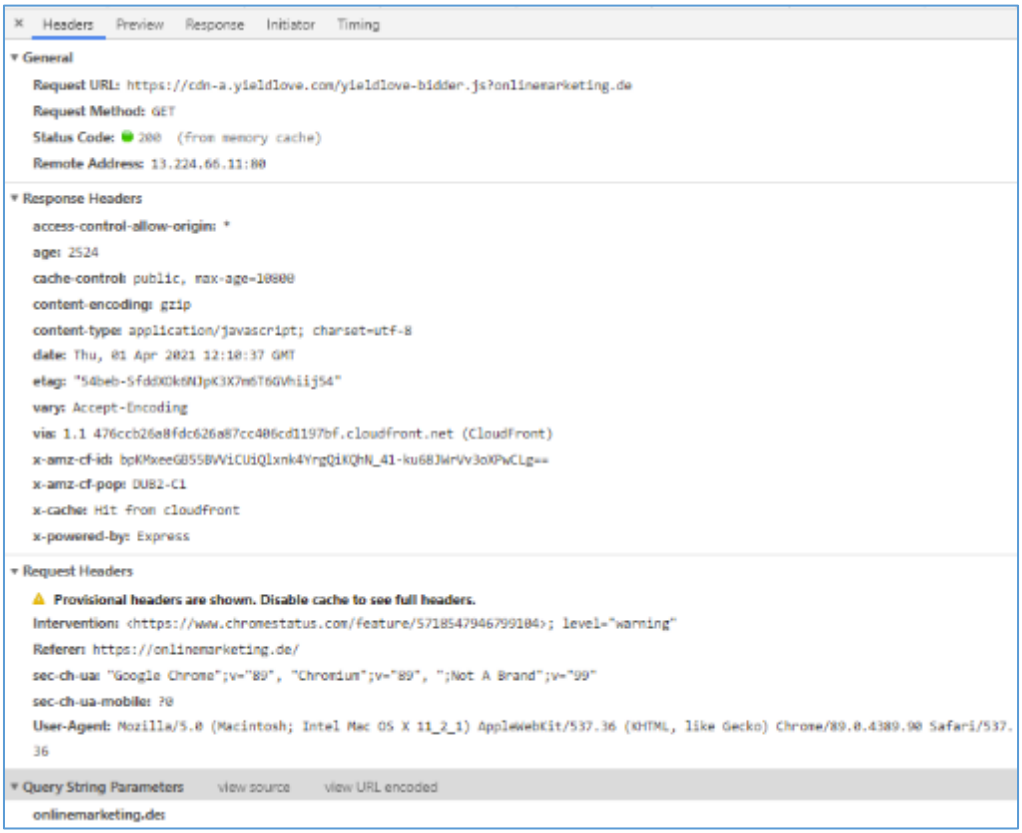


Offer of Proof: Partial printout of presentation slides by Adform's former Senior Product Director Adform Audience Products, Ashu Mathura, available at: https://i.iinfo.cz/files/iac/449/ashu-mathura-adform-1.pdf, last accessed 06/04/2021,

submitted as **Annex K 84**

Adform, moreover, is a member of defendant 1's working group that develops the Audience Taxonomy standard [see Defendant 1's website, Taxonomy & Mapping Working Group, available at https://iabtechlab.com/working-groups/taxonomy-mapping-working-group/, last accessed Apr. 09, 2021].

(4) As already explained in section A. II. 3. a), p. 32, the 3rd defendant used header bidding for the real-time auction of advertising space to maximize the number of companies placing bids for its advertising inventory. As a result of header bidding, each ad slot was routed to multiple SSPs. The (Java)Script "yieldlove-bidder.js" of the provider Yieldlove (Yieldlove GmbH, Kehrwieder 9, 20457 Hamburg) is integrated in the source code of the website of the 3rd defendant. It orchestrates the header bidding, i.e. determines which DSPs are used in which order based on which rules.

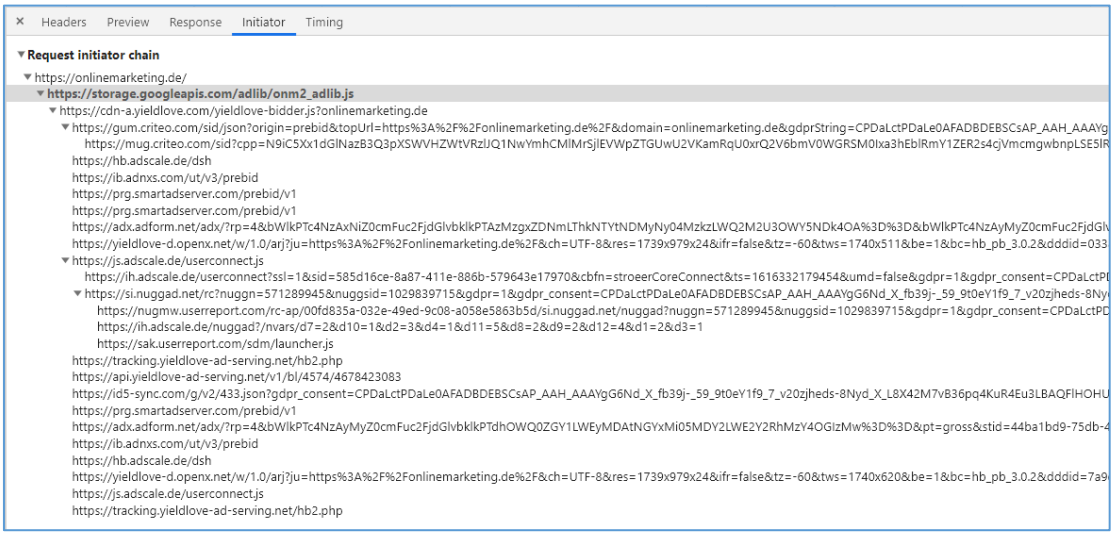


Offer of Proof: Partial printout of website archive file (HAR file) of defendant 3's website dated 04/01/2021 showing network connections (server request) with Yieldlove,

submitted as **Annex K 85**

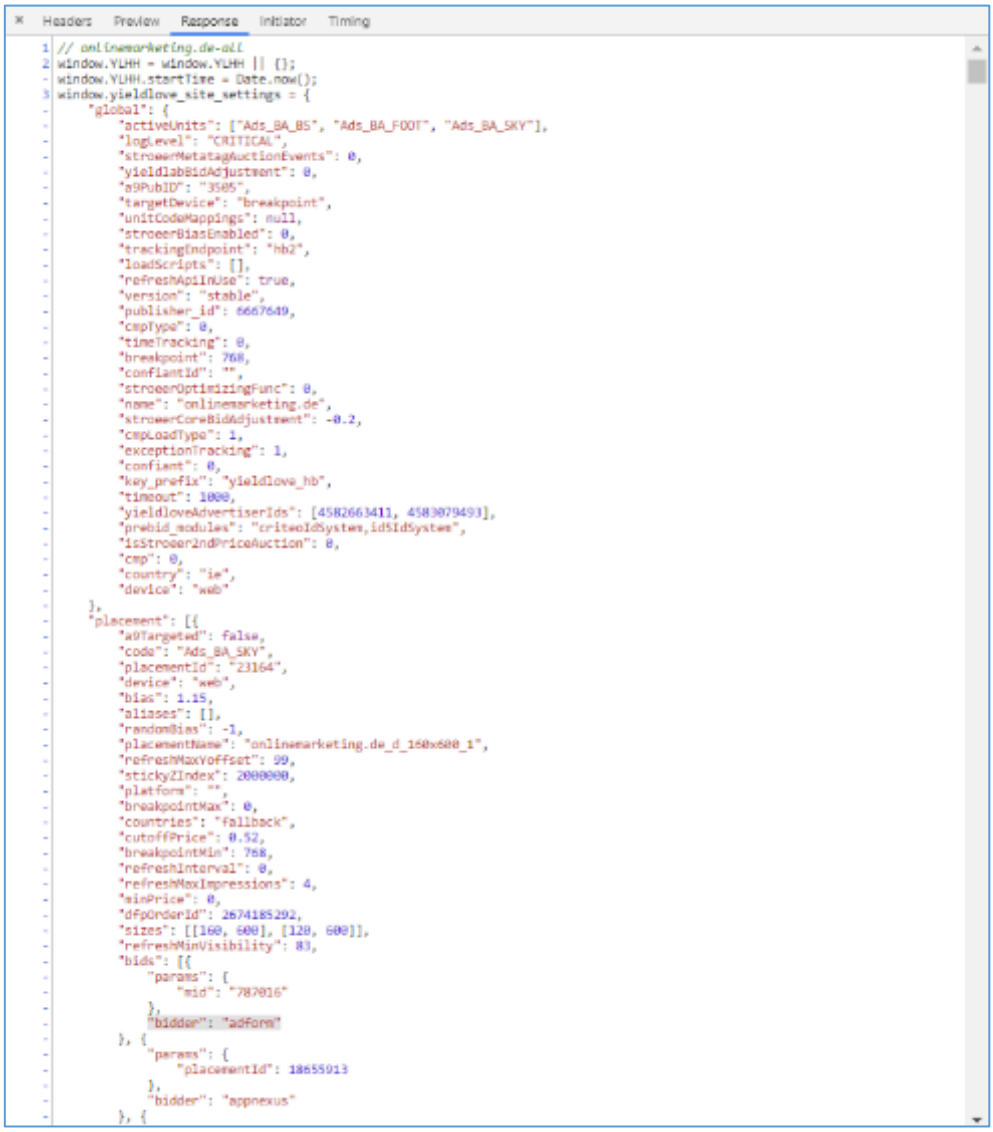
Based on the header bidding script of Yieldlove, the following DSPs were called and all data parameters and personal data of the plaintiff relevant for the execution of the auction were transferred to them, inter alia, to the 2nd defendant:

- Criteo,
- Adscale,
- Xandr (defendant 2),
- Smartadserver,
- Adform,
- OpenX and
- other third-party providers such as NuggAdd and Adscale.



It was established that the technical standard of the 1st defendant OpenRTB was used for the execution of the auctions. Among other things, the relevant server request for the execution of the Real Time Bidding auction was also made to Adform (cf. partial printout of the website archive file (HAR file) of the website of the 3rd defendant dated 25.03.2021 under display of the network connections (server request) with Adform, already submitted as **Annex K 82**).

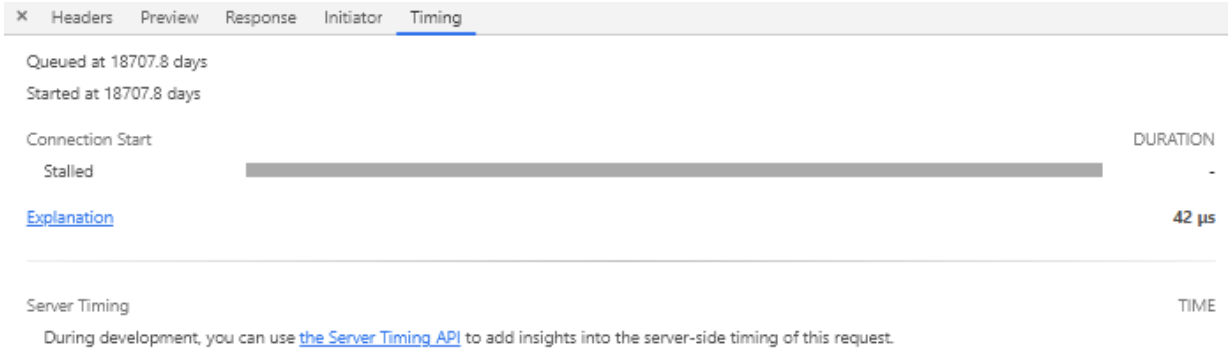
In the process, several bid responses were sent back to Adform from the DSPs, from which details of the real-time auctions conducted can be observed. The server response ("Response") contains unique references to Real Time Bidding auctions ("bidder": "adform", "bid", "prebid modules", "isStroeer2ndPriceAuctionon", "cmp", "cutofPrice": "0.52"), thus evidencing the dissemination of plaintiff's personal data based not only on the OpenRTB technical standard, but also on defendant 1's Content Taxonomy and Audience Taxonomy technical standards when accessing health-related articles on defendant 3's website.



Offer of Proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 04/01/2021 showing the server response with details of the Real Time Bidding auction conducted,

submitted as **Annex K 86**

The execution of the auction on 01.04.2021 with the disclosure of the plaintiff's personal data to an unspecified number of DSPs amounted to 42 milliseconds.



Offer of proof: partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 01.04.2021 showing the duration between server request and server response with details of the Real Time Bidding auction conducted,

presented as **Annex K 87**

2. Processing of particularly sensitive data relating to the applicant

a) Location

According to the legal definition in art. 2 lit. c of Directive 2002/58/EC as amended by Directive 2009/136/EC (hereinafter referred to as the ePrivacy Directive), location data are:

> *"[...] data processed in an electronic communications network indicating the geographical location of the terminal equipment of a user of a publicly available electronic communications service; [...]".*

Recitals 71 and 75 of the ePrivacy Directive confirm the particular sensitivity of location data. The ECJ also emphasized this in the "Child Focus" case [judgment of 06.10.2020, C 511/18 para. 117]:

> *"'[...] traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data 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. In particular, that data provides the means 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 (see, to that effect, judgments of 8 April 2014, Digital Rights, C-293/12 and C-594/12, EU:C:2014:238, paragraph 27, and of 21 December 2016, Tele2, C-203/15 and C-698/15, EU:C:2016:970, paragraph 99).

. "

The location of the data subject can be transmitted in bid requests. Likewise, the IP address may be transmitted, by means of which the location can be determined under certain circumstances. This location information may reveal health or religious affiliation information and is also used for this purpose by companies participating in Real Time Bidding.

For example, UberMedia, a data broker headquartered in California that operates in the EU, has publicly disclosed that it trades data from IAB OpenRTB bid requests. It refers to it as "bid stream" data [UberMedia, SDK Data Impact to the Vista API, available at: [archived]: https://www.iccl.ie/wp-content/uploads/2020/11/SDK_Data_Impact_to_the_Vista_API-UberMedia.pdf], p. 2].

["Bid Stream Data: UberMedia is a marketing demand side platform and participates in ad exchanges, thus collecting data in the process of displaying banner and video ads in over 100,000 apps (~68% of data by volume). This data is also known as RTB data and is collected from an SDK installed by app publishers. […]"

Elsewhere, the company announced that location data from OpenRTB bid requests is accurate to within less than 10 feet. This is equivalent to about 3.05 meters [UberMedia, Location data sources, available at: [archived]: https://www.iccl.ie/wp-content/uploads/2020/11/Location_Data_Sources_One_Sheet-UberMedia.pdf], last accessed 03/23/2021, p. 2].

Company representatives said data from bid requests had a "significant amount of high quality due to scale." The original states [UberMedia, Location data sources, retrieved from: [archived]: https://www.iccl.ie/wp-content/uploads/2020/11/Location_Data_Sources_One_Sheet-UberMedia.pdf], last accessed 03/23/2021]:

"[...] significant amount of high quality due to scale [...]"

In March 2020, UberMedia published a study on how far Italian citizens traveled during the Covid 19 pandemic.

The CEO of UberMedia wrote about OpenRTB data as a source for profiling [*Datta,* A largely ignored but critical dimension to incorporate in understanding consumers on mobile, The Data Source, Oracle, 2016, available at: https://cdn2.hubspot.net/hubfs/4309344/the-data-source-magazine-fall-2016.pdf), last accessed 23/03/2021, p. 22]:

> "[...] Ad requests are not only information-rich, but are also relatively easy to interpret, given the structure imposed on them by standards bodies (such as the IAB OpenRTB organization). [...] Bid requests (BRQs) [...] represent a key source of data [...]".

UberMedia is not alone; Mobilewalla, a Kolkata-based data broker, has publicly stated that the company collects OpenRTB data on individuals and has millions of profiles of devices in the European Union [Mobilewalla, Time: A critical dimension of understanding mobile consumers, presentation hosted at AdSquare.com, March 2017, available at: https://www.adsquare.com/wp-content/uploads/2017/03/08_AIM_Mobilewalla.pdf, last accessed 21/03/2021].

Mobilewalla uses IAB OpenRTB data to profile people over a period of years and analyze where a person is now, how many times they have been to that location before and whether the location is their home, workplace or other location [full listing of information collected: Mobilewalla, Mobilewalla Aggregated Data Dictionary, 2020, available at: https://cdn2.hubspot.net/hubfs/4309344/Content%20Offers/Mobilewalla%20Data%20Dictionary_Aggregated_FEB2020.pdf, last accessed 12/09/2020)]. This allows the company to categorize people as "expectant parents," "dieting and weight loss," "low income," and many more.

The company's CEO revealed in an article that Mobilewalla uses IAB OpenRTB location data to find out people's religious beliefs [*Datta,* A largely ignored but critical dimension to incorporate in understanding consumers on mobile, The Data Source, Oracle, 2016, available at: https://cdn2.hubspot.net/hubfs/4309344/the-data-source-magazine-fall-2016.pdf), last accessed 23/03/2021, p. 22]:

> *"[...] Note that the data elements that enable behavioral persistence identification are already embedded in ad requests-timestamps and location. [...] To identify regular churchgoers, we must figure out which devices have appeared in churches weekly over a period of six months [...]".*

Mobilewalla uses OpenRTB data on a massive scale. An engineer who worked for the company

between 2014 and 2019 [Jiang HaoYuan, https://haoyuan90.github.io/Resume/] said what Mobilewalla had produced:

> "*[...] a data segmentation product [...] on top of collected mobile bid stream data [...]".*

b) Viewed online content

aa) Website currently under consideration

Beyond location data, information about the website or app where an auction is taking place is also transmitted in the bid request, which may constitute special category data. For example, the use of a dating app that targets homosexuals allows conclusions to be drawn about the person's sexual orientation.

bb) Data classified by means of content taxonomy

In addition, bid requests may contain information about what content the data subjects are currently accessing, in the form of tags specified by the 1st defendant's standard content taxonomy. Categories are used from which the political opinion, religion, health data or sexuality of the data subject can be inferred.

Defendant 1 has publicly acknowledged that Content Taxonomy discloses special category data and has adopted the acronym "SCD" ("Special Category Data") to identify it,

> "*[...] to minimize the risk that content categorization signals within Open RTB (Real Time Bidding) requests could be used to generate sensitive data points about things like race, politics, religion or other personal characteristics that could result in discrimination. [...]"*

Offer of Proof: Entire printout of 1st defendant's website, Final Audience Taxonomy v1.1 and Content Taxonomy v2.1 provide additional consumer privacy safeguards, as amended 09/07/2020, available at: https://iabtechlab.com/blog/final-audience-content-taxonomies-provide-additional-consumer-privacy-safeguards/, last accessed 03/24/2021,

submitted as **Annex K 88**

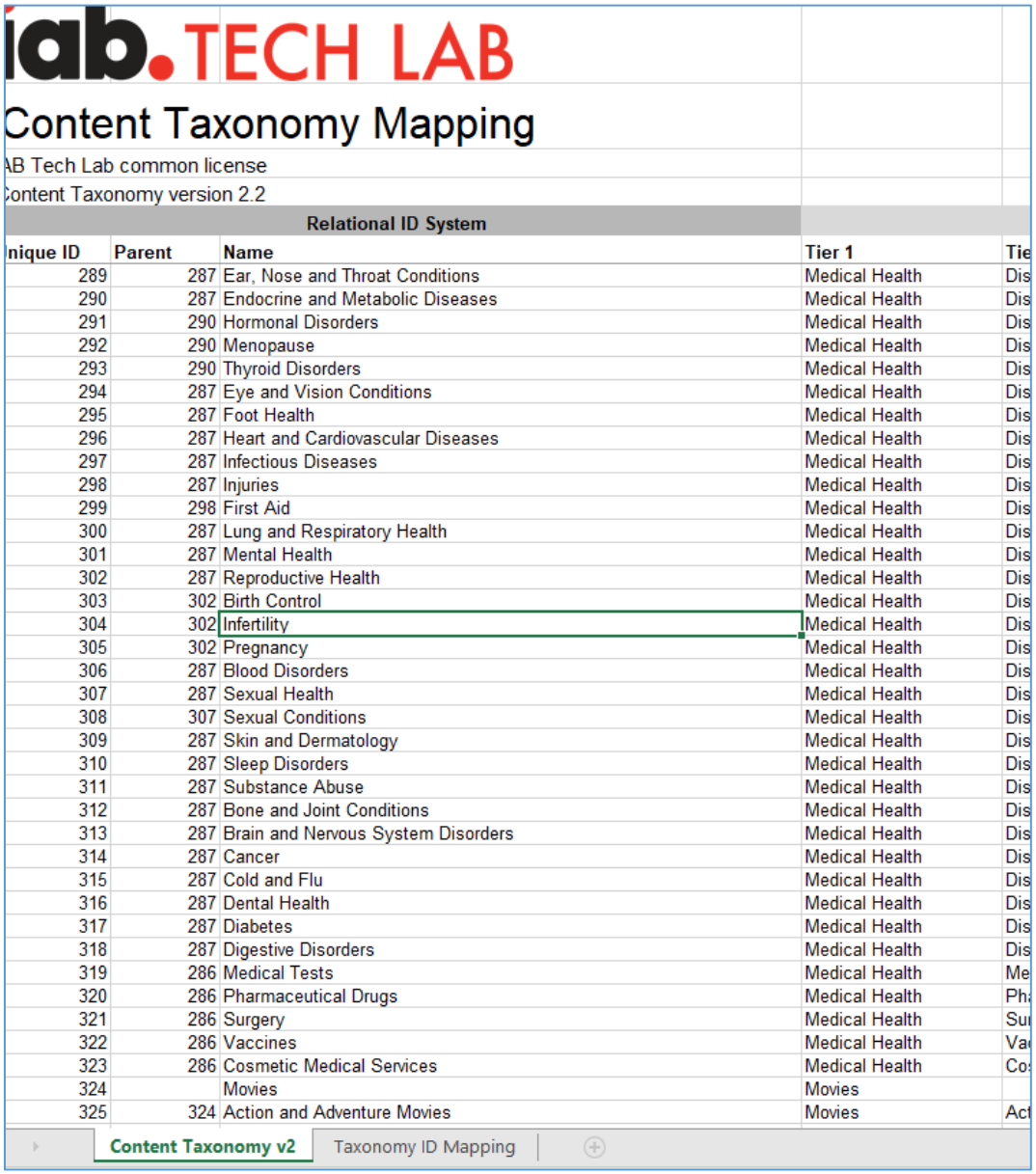
However, the 1st defendant has confirmed that the addition of the abbreviation to the relevant categories of the standard does not mean that data of this type will no longer be processed. Its senior manager Benjamin Dick, on the other hand, wrote to the plaintiff in an email dated 27.08.2020:

"[...] the SCD flag is a marker that those categories should be treated with special consideration [...]".

Offer of Proof: Printout of email from Benjamin Dick to plaintiff dated 8/27/2020,

submitted as **Annex K 89**

The table below shows some of the interests included in the Content Taxonomy v2.2 standard for distribution in OpenRTB bid requests. For example, "Mental Health", "Infertility", "Cancer" and "Substance Abuse" are included.



iab. TECH LAB

Content Taxonomy Mapping

AB Tech Lab common license

ontent Taxonomy version 2.2

		Relational ID System		
nique ID	Parent	Name	Tier 1	Tie
289	287	Ear, Nose and Throat Conditions	Medical Health	Dis
290	287	Endocrine and Metabolic Diseases	Medical Health	Dis
291	290	Hormonal Disorders	Medical Health	Dis
292	290	Menopause	Medical Health	Dis
293	290	Thyroid Disorders	Medical Health	Dis
294	287	Eye and Vision Conditions	Medical Health	Dis
295	287	Foot Health	Medical Health	Dis
296	287	Heart and Cardiovascular Diseases	Medical Health	Dis
297	287	Infectious Diseases	Medical Health	Dis
298	287	Injuries	Medical Health	Dis
299	298	First Aid	Medical Health	Dis
300	287	Lung and Respiratory Health	Medical Health	Dis
301	287	Mental Health	Medical Health	Dis
302	287	Reproductive Health	Medical Health	Dis
303	302	Birth Control	Medical Health	Dis
304	302	Infertility	Medical Health	Dis
305	302	Pregnancy	Medical Health	Dis
306	287	Blood Disorders	Medical Health	Dis
307	287	Sexual Health	Medical Health	Dis
308	307	Sexual Conditions	Medical Health	Dis
309	287	Skin and Dermatology	Medical Health	Dis
310	287	Sleep Disorders	Medical Health	Dis
311	287	Substance Abuse	Medical Health	Dis
312	287	Bone and Joint Conditions	Medical Health	Dis
313	287	Brain and Nervous System Disorders	Medical Health	Dis
314	287	Cancer	Medical Health	Dis
315	287	Cold and Flu	Medical Health	Dis
316	287	Dental Health	Medical Health	Dis
317	287	Diabetes	Medical Health	Dis
318	287	Digestive Disorders	Medical Health	Dis
319	286	Medical Tests	Medical Health	Me
320	286	Pharmaceutical Drugs	Medical Health	Ph
321	286	Surgery	Medical Health	Su
322	286	Vaccines	Medical Health	Va
323	286	Cosmetic Medical Services	Medical Health	Co
324		Movies	Movies	
325	324	Action and Adventure Movies	Movies	Act

Content Taxonomy v2 | Taxonomy ID Mapping

Offer of Proof: Partial printout of 1st defendant's Protocol technical specifications, Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/standards/content-taxonomy/, last accessed 03/22/2021,

submitted as **Annex K 90**

There are also categories related to the user's religion:

iab. TECH LAB

Content Taxonomy Mapping

IAB Tech Lab common license

Content Taxonomy version 2.2

Relational ID System				
Unique ID	Parent	Name	Tier 1	Tier 2
443	441	Retail Property	Real Estate	Retail Property
444	441	Vacation Properties	Real Estate	Vacation Properties
445	441	Developmental Sites	Real Estate	Developmental Sites
446	441	Hotel Properties	Real Estate	Hotel Properties
447	441	Houses	Real Estate	Houses
448	441	Industrial Property	Real Estate	Industrial Property
449	441	Land and Farms	Real Estate	Land and Farms
450	441	Office Property	Real Estate	Office Property
451	441	Real Estate Buying and Selling	Real Estate	Real Estate Buying and Selli
452	441	Real Estate Renting and Leasing	Real Estate	Real Estate Renting and Leas
453		Religion & Spirituality	Religion & Spirituality	
454	453	Agnosticism	Religion & Spirituality	Agnosticism
455	453	Spirituality	Religion & Spirituality	Spirituality
456	453	Astrology	Religion & Spirituality	Astrology
457	453	Atheism	Religion & Spirituality	Atheism
458	453	Buddhism	Religion & Spirituality	Buddhism
459	453	Christianity	Religion & Spirituality	Christianity
460	453	Hinduism	Religion & Spirituality	Hinduism
461	453	Islam	Religion & Spirituality	Islam
462	453	Judaism	Religion & Spirituality	Judaism
463	453	Sikhism	Religion & Spirituality	Sikhism
464		Science	Science	
465	464	Biological Sciences	Science	Biological Sciences
466	464	Chemistry	Science	Chemistry
467	464	Environment	Science	Environment
468	464	Genetics	Science	Genetics
469	464	Geography	Science	Geography
470	464	Geology	Science	Geology
471	464	Physics	Science	Physics
472	464	Space and Astronomy	Science	Space and Astronomy

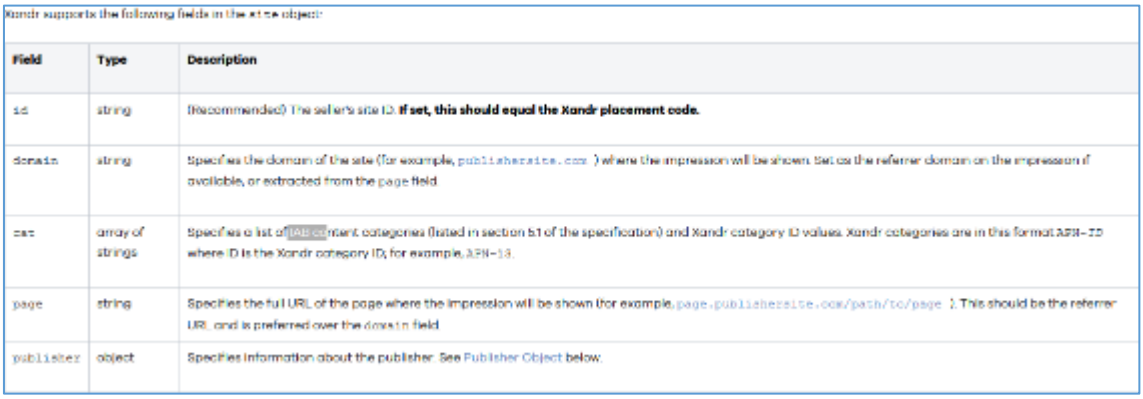
Offer of Proof: Partial printout of 1st defendant's Protocol technical specifications, Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/standards/content-taxonomy/, last accessed 03/22/2021,

submitted as **Annex K 91**

Offer of Proof: Full printout of 1st defendant's Protocol technical specification, Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/standards/content-taxonomy/, last accessed 03/22/2021,

submitted as **Annex K 92**

Defendant 2 itself acknowledges that it uses defendant 1's Content Taxonomy.



Xandr supports the following fields in the `site` object:

Field	Type	Description
`id`	string	(Recommended) The seller's site ID. **If set, this should equal the Xandr placement code.**
`domain`	string	Specifies the domain of the site (for example, `publishersite.com`) where the impression will be shown. Set as the referrer domain on the impression if available, or extracted from the `page` field.
`cat`	array of strings	Specifies a list of IAB content categories (listed in section 5.1 of the specification) and Xandr category ID values. Xandr categories are in this format: `XPR-ID` where ID is the Xandr category ID, for example, `XPR-13`.
`page`	string	Specifies the full URL of the page where the impression will be shown (for example, `page.publishersite.com/path/to/page`). This should be the referrer URL and is preferred over the `domain` field.
`publisher`	object	Specifies information about the publisher. See Publisher Object below.

Offer of Proof: Partial printout of 2nd defendant's website, Incoming Bid Request from SSPs, as amended 06/04/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed 06/04/2021,

submitted as **Annex K 93**

Defendant 1's Content Taxonomy is used, for example, by a data broker company called "OnAudience". The company offers for sale personal profiles of over 200 individuals in Ireland categorized as interested in "Incest & Abuse Support" [OnAudience: Audience Taxonomy, formerly available at: https://www.onaudience.com/taxonomy/ireland, last accessed on: 09/15/2020, OnAudience recently removed this information from their website]. This category comes from defendant 1's standard Content Taxonomy. OnAudience states that it uses standards of the 1st defendant [Oracle Data Cloud: "OnAudience.com: a buyers guide", available at: http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf, last accessed on 07.04.2021, p. 109].

Furthermore, OnAudience offers 100 profiles of people from the category "Brain Tumor", 1,300 with the attribute "AIDS & HIV" and 1,200 people to the category "Substance Abuse." [archived screenshots available at: https://www.iccl.ie/wp-content/uploads/2020/11/screencapture-onaudience-taxonomy-ireland-2020-09-15-06_25_49.png and at: https://www.iccl.ie/wp-content/uploads/2020/11/screencapture-onaudience-taxonomy-ireland-2020-09-15-06_25_49-2.png].

OnAudience stated that it collects data from DSPs that receive OpenRTB bid requests from Advertising Exchanges such as defendant 2 or data from Oracle Data Cloud [OnAudience.com,

Oracle Audiences: A buyers guide, available at: http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf, last accessed 07/04/2021, p. 110]:

> *"[...] We analyze more than several billion impressions daily working closely with DSP and DMP partners [...].*

Defendant 3 allows both OnAudience and Oracle Data Cloud to have a presence on its website.

This allows these companies to build profiles by constantly monitoring website views as well as viewed website content:

> *"[...] observing [...] websites visited, content consumed and history paths to find clear behavior patterns and proper level of intent" [...].*

The Article 29 Working Party has confirmed [Art. 29 Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev. 01] that special category data are involved:

> *"[...] 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. [...]"*

Incidentally, data that refer to an individual but are inaccurate also constitute personal data. Otherwise, the right of rectification under art. 16 GDPR would have no scope.

According to a case study published by OnAudience, the company profiled over 1.4 million people to influence the 2019 Polish general election. Through data obtained via OpenRTB, they built profiles on these people's sexuality and political views [OnAudience, Creating custom segments for "I vote for love" campaign, p. 1, archived available at: http://web.archive.org/web/20201004015441/https://www.onaudience.com/files/Case-Study-VMLYR-OnAudience.pdf, last accessed on 2020-09-15].

cc) Data classified by means of audience taxonomy

Finally, "segments" can also be transmitted with a bid request, which classify the website or app user as such into categories. These segments originate from the standard Audience Taxonomy of the 1st defendant. This is stated in a communication of the 1st defendant:

"[...] With the introduction of IAB Tech Lab's Audience Taxonomy 1.0, the industry now has a common nomenclature for audience segment names to improve comparability of data across different providers. [...]"

Audience Taxonomy, according to the 1st defendant, is to be used as part of OpenRTB so that DSPs (DSPs) receive the segment identifier with the bid requests and make appropriate allocations:

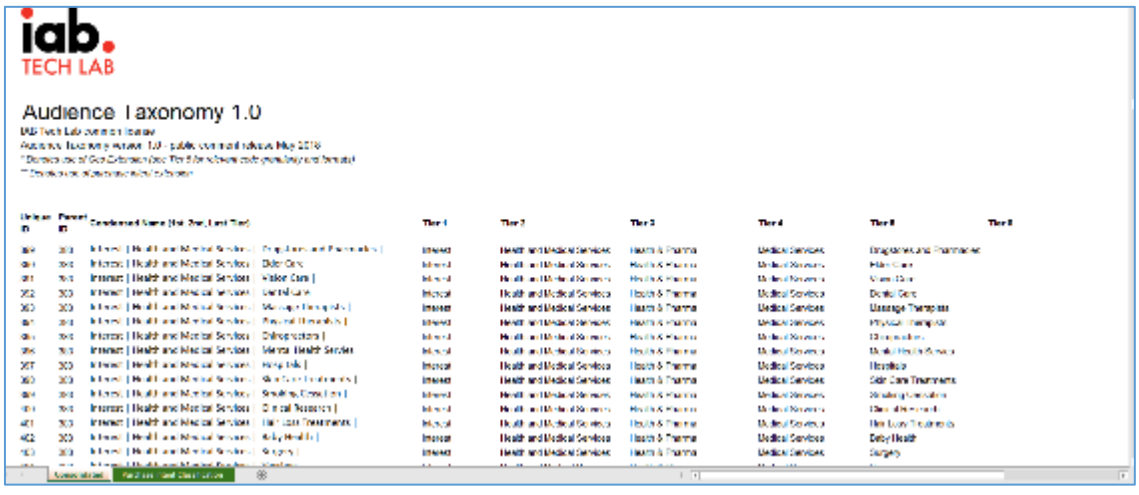
["Sophisticated DSPs will be able to adjust weighting / frequency of use for different audience segments and vendors in real-time. DSPs will also be able to adjust the price paid for data and / or bid prices for audience + media packages, using the taxonomy to compare similar segment performance across vendors. [...]"

Offer of Proof: Entire printout of 1st defendant's website, Audience Taxonomy, as amended April 2020, available at: https://iabtechlab.com/standards/audience-taxonomy/, last accessed 03/24/2021,

submitted as **Annex K 94**

Audience Taxonomy is used to categorize people into segments based on their individual characteristics. Version 1.0 includes 1,679 attributes that can be added to people's profiles.

Here are some examples that relate to health status:

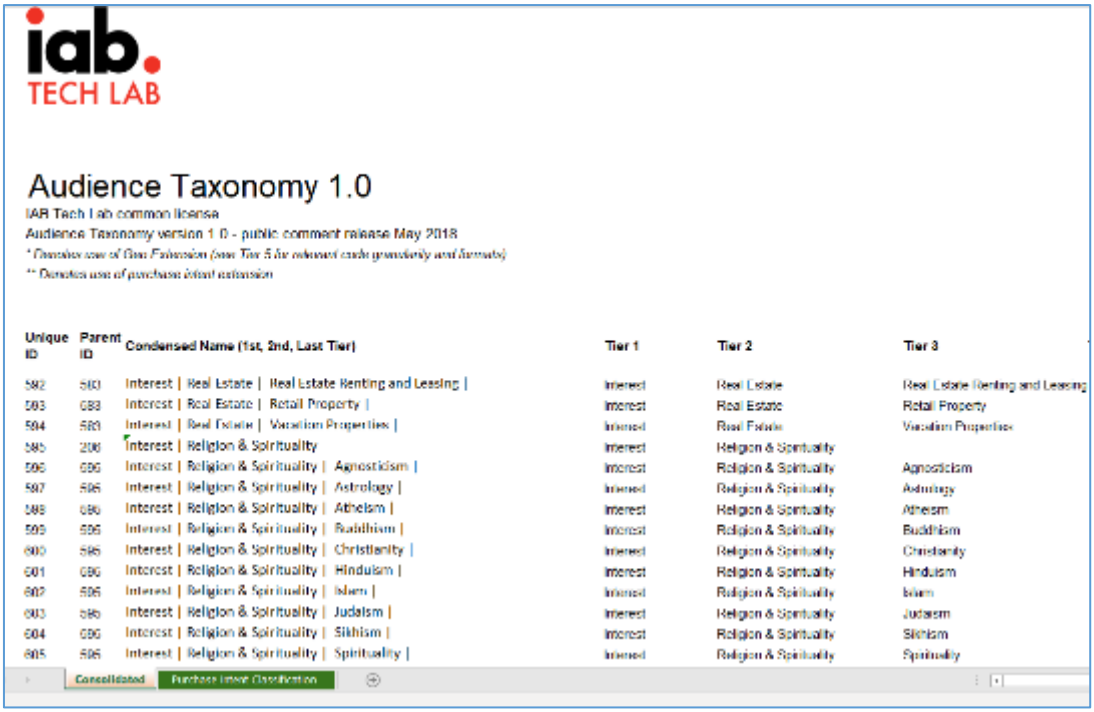


Offer of Proof: Partial printout of 1st defendant's Protocol technical specifications, Audience Taxonomy v1.0, as amended May 2018, available at:

https://iabtechlab.com/standards/audience-taxonomy/, last accessed 03/23/2021,

submitted as **Annex K 95**

Audience Taxonomy also provides attributes related to religious affiliation:



iab. TECH LAB

Audience Taxonomy 1.0

IAB Tech Lab common license

Audience Taxonomy version 1.0 - public comment release May 2018

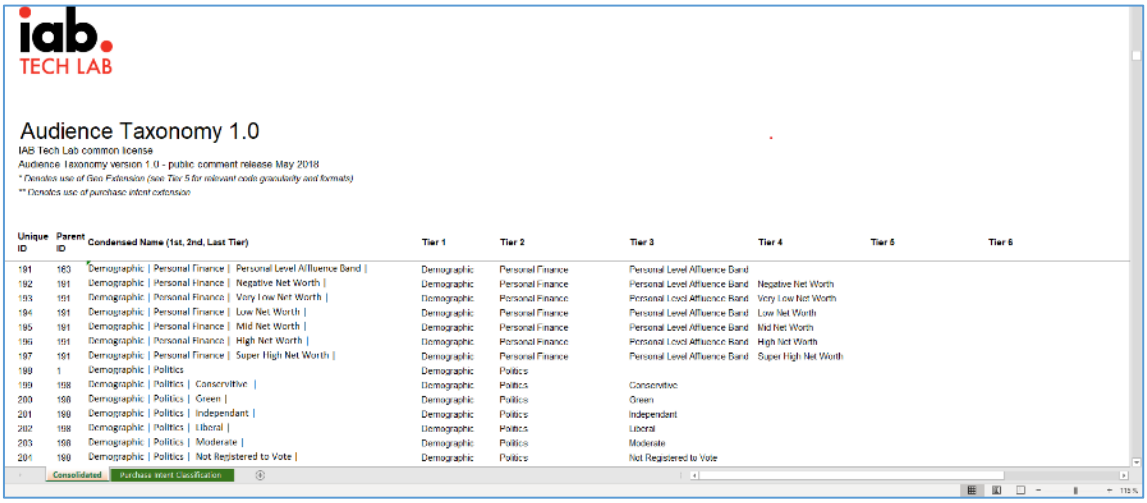
Unique ID	Parent ID	Condensed Name (1st, 2nd, Last Tier)	Tier 1	Tier 2	Tier 3
582	580	Interest | Real Estate | Real Estate Renting and Leasing |	Interest	Real Estate	Real Estate Renting and Leasing
583	580	Interest | Real Estate | Retail Property |	Interest	Real Estate	Retail Property
584	580	Interest | Real Estate | Vacation Properties |	Interest	Real Estate	Vacation Properties
585	206	Interest | Religion & Spirituality	Interest	Religion & Spirituality	
586	586	Interest | Religion & Spirituality | Agnosticism |	Interest	Religion & Spirituality	Agnosticism
587	586	Interest | Religion & Spirituality | Astrology |	Interest	Religion & Spirituality	Astrology
588	586	Interest | Religion & Spirituality | Atheism |	Interest	Religion & Spirituality	Atheism
589	586	Interest | Religion & Spirituality | Buddhism |	Interest	Religion & Spirituality	Buddhism
590	586	Interest | Religion & Spirituality | Christianity |	Interest	Religion & Spirituality	Christianity
591	586	Interest | Religion & Spirituality | Hinduism |	Interest	Religion & Spirituality	Hinduism
592	586	Interest | Religion & Spirituality | Islam |	Interest	Religion & Spirituality	Islam
593	586	Interest | Religion & Spirituality | Judaism |	Interest	Religion & Spirituality	Judaism
594	586	Interest | Religion & Spirituality | Sikhism |	Interest	Religion & Spirituality	Sikhism
595	586	Interest | Religion & Spirituality | Spirituality |	Interest	Religion & Spirituality	Spirituality

Consolidated | Purchase Intent Classification

Offer of Proof: Partial printout of 1st defendant's Protocol technical specifications, Audience Taxonomy v1.0, dated 2018, available at: https://iabtechlab.com/standards/audience-taxonomy/ last accessed 03/23/2021,

submitted as **Annex K 96**

In addition to information on the financial situation of the website visitor, Audience Taxonomy v1.0 also contains information on political preferences, which can be used to influence advertisements in the run-up to an democratic election.



iab. TECH LAB

Audience Taxonomy 1.0

IAB Tech Lab common license

Audience Taxonomy version 1.0 - public comment release May 2018

* Denotes use of Geo Extension (see Tier 5 for relevant code granularity and formats)

** Denotes use of purchase intent extension

Unique ID	Parent ID	Condensed Name (1st, 2nd, Last Tier)	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6
191	183	Demographic | Personal Finance | Personal Level Affluence Band |	Demographic	Personal Finance	Personal Level Affluence Band			
192	191	Demographic | Personal Finance | Negative Net Worth |	Demographic	Personal Finance	Personal Level Affluence Band	Negative Net Worth		
193	191	Demographic | Personal Finance | Very Low Net Worth |	Demographic	Personal Finance	Personal Level Affluence Band	Very Low Net Worth		
194	191	Demographic | Personal Finance | Low Net Worth |	Demographic	Personal Finance	Personal Level Affluence Band	Low Net Worth		
195	191	Demographic | Personal Finance | Mid Net Worth |	Demographic	Personal Finance	Personal Level Affluence Band	Mid Net Worth		
196	191	Demographic | Personal Finance | High Net Worth |	Demographic	Personal Finance	Personal Level Affluence Band	High Net Worth		
197	191	Demographic | Personal Finance | Super High Net Worth |	Demographic	Personal Finance	Personal Level Affluence Band	Super High Net Worth		
198	1	Demographic | Politics	Demographic	Politics				
199	198	Demographic | Politics | Conservative |	Demographic	Politics	Conservative			
200	198	Demographic | Politics | Green |	Demographic	Politics	Green			
201	198	Demographic | Politics | Independant |	Demographic	Politics	Independant			
202	198	Demographic | Politics | Liberal |	Demographic	Politics	Liberal			
203	198	Demographic | Politics | Moderate |	Demographic	Politics	Moderate			
204	198	Demographic | Politics | Not Registered to Vote |	Demographic	Politics	Not Registered to Vote			

Consolidated | Purchase Intent Classification

Offer of Proof: Partial printout of 1st defendant's Protocol technical specifications, Audience Taxonomy v1.0, as amended May 2018, available at: https://iabtechlab.com/standards/audience-taxonomy/, last accessed 03/23/2021,

submitted as **Annex K 97**

Offer of Proof: Entire printout of 1st defendant's Protocol technical specifications, Audience Taxonomy v1.0, as amended May 2018, available at: https https://iabtechlab.com/standards/audience-taxonomy/, last accessed 03/29/2021,

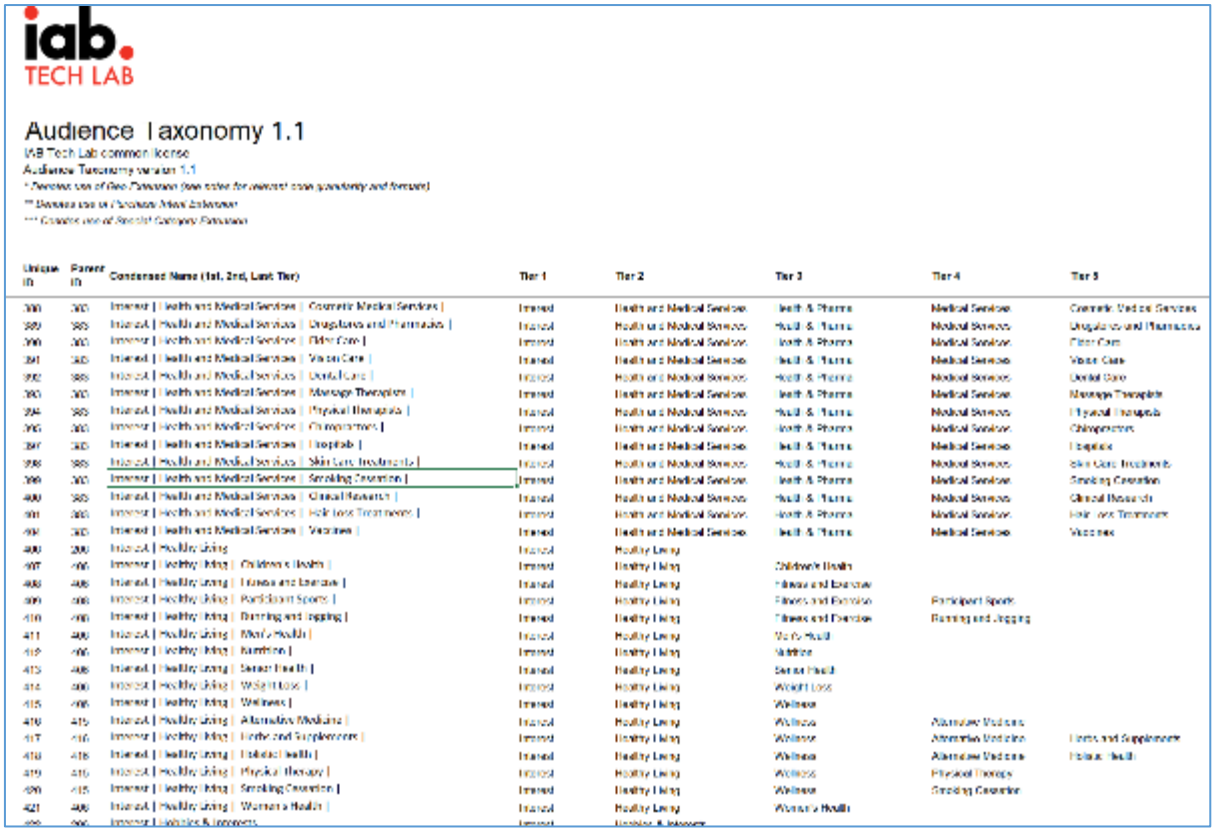
presented as **Annex K 98**

A new version also exists (Audience Taxonomy v1.1.), in which some of these particularly sensitive attributions have been removed, but not the majority. Both versions are available for download on the website of defendant 1.

Categories are included that describe health, debt, crime, political views, and religious affiliation. There are also categories that describe personal wealth. For example:

- Personal wealth: very low net wealth (IAB code 193), debts (IAB code 537)
- Household: rural (IAB code 147)

- Personal interests: Vaccinations (IAB code 404)
- Health related issues: Weight loss (IAB code 414)



iab.
TECH LAB

Audience Taxonomy 1.1

IAB Tech Lab common license

Audience Taxonomy version 1.1

Unique ID	Parent ID	Concatenated Name (1st, 2nd, Last Tier)	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
389	385	Interest | Health and Medical Services | Cosmetic Medical Services	Interest	Health and Medical Services	Health & Pharma	Medical Services	Cosmetic Medical Services
389	385	Interest | Health and Medical Services | Drugstores and Pharmacies	Interest	Health and Medical Services	Health & Pharma	Medical Services	Drugstores and Pharmacies
390	385	Interest | Health and Medical Services | Elder Care	Interest	Health and Medical Services	Health & Pharma	Medical Services	Elder Care
391	385	Interest | Health and Medical Services | Vision Care	Interest	Health and Medical Services	Health & Pharma	Medical Services	Vision Care
392	385	Interest | Health and Medical Services | Dental Care	Interest	Health and Medical Services	Health & Pharma	Medical Services	Dental Care
393	385	Interest | Health and Medical Services | Massage Therapists	Interest	Health and Medical Services	Health & Pharma	Medical Services	Massage Therapists
394	385	Interest | Health and Medical Services | Physical Therapists	Interest	Health and Medical Services	Health & Pharma	Medical Services	Physical Therapists
395	385	Interest | Health and Medical Services | Chiropractors	Interest	Health and Medical Services	Health & Pharma	Medical Services	Chiropractors
397	385	Interest | Health and Medical Services | Hospitals	Interest	Health and Medical Services	Health & Pharma	Medical Services	Hospitals
398	385	Interest | Health and Medical Services | Skin Care Treatments	Interest	Health and Medical Services	Health & Pharma	Medical Services	Skin Care Treatments
399	385	Interest | Health and Medical Services | Smoking Cessation	Interest	Health and Medical Services	Health & Pharma	Medical Services	Smoking Cessation
400	385	Interest | Health and Medical Services | Clinical Research	Interest	Health and Medical Services	Health & Pharma	Medical Services	Clinical Research
401	385	Interest | Health and Medical Services | Hair Loss Treatments	Interest	Health and Medical Services	Health & Pharma	Medical Services	Hair Loss Treatments
402	385	Interest | Health and Medical Services | Vaccines	Interest	Health and Medical Services	Health & Pharma	Medical Services	Vaccines
406	406	Interest | Healthy Living	Interest	Healthy Living			
407	406	Interest | Healthy Living | Children's Health	Interest	Healthy Living	Children's Health		
408	406	Interest | Healthy Living | Fitness and Exercise	Interest	Healthy Living	Fitness and Exercise		
409	406	Interest | Healthy Living | Participant Sports	Interest	Healthy Living	Fitness and Exercise	Participant Sports	
410	406	Interest | Healthy Living | Running and Jogging	Interest	Healthy Living	Fitness and Exercise	Running and Jogging	
411	406	Interest | Healthy Living | Men's Health	Interest	Healthy Living	Men's Health		
412	406	Interest | Healthy Living | Nutrition	Interest	Healthy Living	Nutrition		
413	406	Interest | Healthy Living | Senior Health	Interest	Healthy Living	Senior Health		
414	406	Interest | Healthy Living | Weight Loss	Interest	Healthy Living	Weight Loss		
415	406	Interest | Healthy Living | Wellness	Interest	Healthy Living	Wellness		
416	415	Interest | Healthy Living | Alternative Medicine	Interest	Healthy Living	Wellness	Alternative Medicine	
417	416	Interest | Healthy Living | Herbs and Supplements	Interest	Healthy Living	Wellness	Alternative Medicine	Herbs and Supplements
418	416	Interest | Healthy Living | Holistic Health	Interest	Healthy Living	Wellness	Alternative Medicine	Holistic Health
419	415	Interest | Healthy Living | Physical Therapy	Interest	Healthy Living	Wellness	Physical Therapy	
420	415	Interest | Healthy Living | Smoking Cessation	Interest	Healthy Living	Wellness	Smoking Cessation	
421	406	Interest | Healthy Living | Women's Health	Interest	Healthy Living	Women's Health		
422	422	Interest | Logistics & Transport	Interest	Logistics & Transport			

Offer of Proof: Partial printout of 1st defendant's Protocol technical specifications, Audience Taxonomy v1.1, as amended April 2020, available at: https://iabtechlab.com/standards/audience-taxonomy/, last accessed 03/24/2021,

submitted as **Annex K 99**

Offer of Proof: Entire printout of 1st defendant's Protocol technical specification, Audience Taxonomy v1.1, as amended April 2020, available at https://iabtechlab.com/standards/audience-taxonomy/, last accessed Feb. 12, 2021,

presented as **Annex K 100**

The 2nd defendant admits that it only accepts bid requests from SSPs if a "Xandr user ID" is included in order to enable "segment targeting", i.e. the use of categories from the 1st defendant's technical standard (cf. already point A. II. 2. d), p. 28) for the placement of advertisements [cf. partial printout of the 2nd defendant's website, Documentation Center: User ID Mapping, available at: https://docs.xandr.com/bundle/supply-partners/page/user-id-mapping.html, last accessed on 25.03.2021, already submitted as **Annex K 78**].

> "*[...] When you send Xandr a bid request, Xandr responds with a bid only when we can map your request to a Xandr user ID. Without this user ID, we can't apply basic trafficking strategies for our advertisers, such as user frequency capping and segment targeting. [...]".*

c) Consent String Record

As described in section A. II. 1. (p. 15), an identifier called a Consent String is sent with a bid request.

The Consent String is a unique identifier about a person that records which websites and apps they have used. For example, the consent string records whether a person uses a gay dating app, a Bible app, reads conservative online newspapers, or visits cancer forums or union websites.

The following data is contained in the Consent String:

- A permanent record of the exact time (to within a tenth of a second) and date that the TCF Consent String was first created about the individual (this timestamp is highly likely to be unique to each individual);
- Language of the person;
- the country in which the website being viewed is hosted;
- The options the individual selected in the TCF Consent & Transparency Notices;
- the version of the Consent Management Platform;
- the exact time (to a tenth of a second) and date when the record was last modified. This allows anyone with access to the Consent String to add new data about the person.

The Core String

The following fields are stored in big-endian format. Bit numberings are left-to-right.

Field Name	Bits	Value(s)	Notes
Version	6 bits	Version number of the encoding format.	The value is 2 for this format.
Created	36 bits	Epoch deciseconds when the TC String was first created (should not be changed unless a new TCString is created from scratch)	A decisecond is 1/10th of a second. To create a deciseconds timestamp in JavaScript: `Math.round(new Date().getTime()/100)`
LastUpdated	36 bits	Epoch deciseconds when TC String was last updated (Must be updated any time a value is changed)	
CmpId	12 bits	Consent Management Platform ID that last updated the TC String	A unique ID will be assigned to each Consent Management Platform.
CmpVersion	12 bits	Consent Management Platform version of the CMP that last updated this TC String	Each change to a CMP should increment their internally assigned version number as a record of which version the user gave consent and transparency was established.
ConsentScreen	6 bits	CMP Screen number at which consent was given for a user with the CMP that last updated this TC String	The number is a CMP internal designation and is CmpVersion specific. The number is used for identifying on which screen a user gave consent as a record.
ConsentLanguage	12 bits	Two-letter ISO 639-1 language code in which the CMP UI was presented	Each letter is encoded as 6 bits, a=0,z=25.
VendorListVersion	12 bits	Number corresponds to GVL `vendorListVersion`	Version of the GVL used to create the TC String.
TcfPolicyVersion	6 bits	Version of policy used with in GVL	From the corresponding field in the GVL that was used for obtaining consent. A new policy version invalidates existing strings and requires CMPs to re-establish transparency and consent from users.
IsServiceSpecific	1 bit	1: True 0: False	Whether the signals encoded in this TC String were from service specific storage (true) versus "global" consent using shared storage (false)
UseNonStandardStacks	1 bit	1: CMP used non-IAB standard stacks during consent gathering 0: IAB standard stacks were used	Setting this to 1 means that a publisher-run CMP – that is still IAB Europe registered – is using publisher-specific descriptions and not the standard stack descriptions defined in the Policies (Appendix A section F). A CMP that services multiple publishers sets this value to 0.
SpecialFeatureOptins	12 bits	One bit for each Special Feature 1: Opted in 0: Not opted in	The TCF Policies designates certain features as "special" which means a CMP must afford the user a means to opt in to their use. These "Special Features" are published and numerically identified in the Global Vendor List separately from normal features.
PurposesConsent (generated from PurposesAllowed)	24 bits	One bit for each Purpose 1: Consent 0: No Consent	The user's consent value for each Purpose established on the legal basis of consent. The Purposes are numerically identified and published in the Global Vendor List. From left to right, Purpose 1 maps to the 0th bit, purpose 24 maps to the bit at index 23. Special Purposes are a different ID space and not included in this field.
PurposesLITransparency	24 bits	One bit for each Purpose 1: legitimate interest established 0: legitimate interest was NOT established or it was established but user exercised their "right to Object" to the Purpose	The Purpose's transparency requirements are met for each Purpose on the legal basis of legitimate interest and the user has not exercised their "Right to Object" to that Purpose. By default or if the user has exercised their "Right to Object" to a Purpose, the corresponding bit for that Purpose is set to 0. From left to right, Purpose 1 maps to the 0th bit, purpose 24 maps to the bit at index 23. Special Purposes are a different ID space and not included in this field.
Specific Jurisdiction Disclosures			
PurposeOneTreatment	1 bit	1: Purpose 1 was NOT disclosed at all. 0: Purpose 1 was disclosed commonly as consent as expected by the Policies.	CMPs can use the PublisherCC field to indicate the legal jurisdiction the publisher is under to help vendors determine whether the vendor needs consent for Purpose 1. In a globally-scoped TC string, this field must always have a value of 0. When a CMP encounters a globally-scoped TC String with PurposeOneTreatment=1 then it is considered invalid and the CMP must discard it and re-establish transparency and consent.
PublisherCC	12 bits	ISO 3166-1 alpha-2 code	The country code of the country that determines legislation of reference. Commonly, this corresponds to the country in which the publisher's business entity is established. Each letter is encoded as 6 bits, a=0,z=25.
Vendor Consent Section			
MaxVendorId	16 bits	The maximum Vendor ID that is represented in the following bit field or range encoding.	Because this section can be a variable length, this indicates the last ID of this section so that a decoder will know when it has reached the end.
IsRangeEncoding	1 bit	1: Range 0: BitField	The encoding scheme used to encode the IDs in the section – Either a BitField Section or Range Section follows. Encoding logic should choose the encoding scheme that results in the smaller output size for a given set.

Offer of Proof: Partial Printout of 1st defendant's Technical Specification, Transparency and Consent String with Global Vendor & CMP List Format, as amended December 2019, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#the-core-string, last accessed 03/24/2021,

submitted as **Annex K 101**

Offer of Proof: Entire Printout of 1st defendant's Technical Specification, Transparency and Consent String with Global Vendor & CMP List Format, as amended December 2019, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md, last accessed 03/29/2021,

submitted as **Annex K 102**

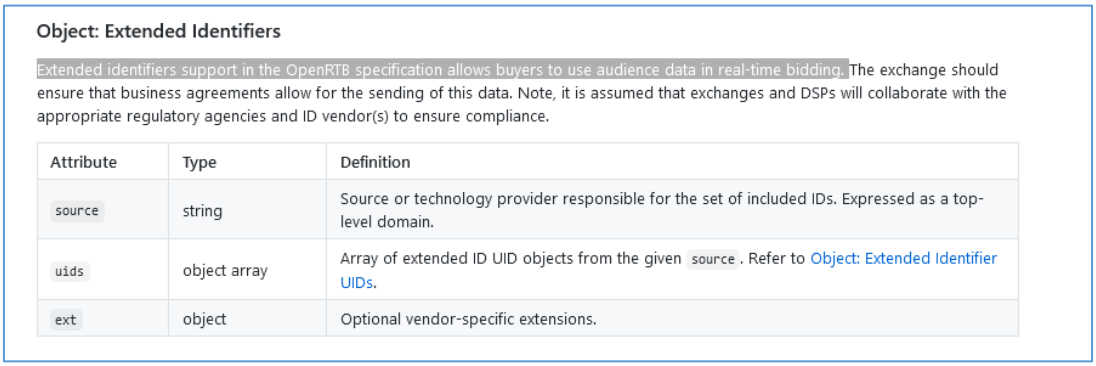
The underlying Transparency & Consent Framework is used for 80% of such activities in Europe, so the overview of the Internet usage behaviour of the data subjects is likely to provide very intimate insights.

d) Extensions

As shown in A.II.1, OpenRTB bid requests also include "extensions".

This allows additional personal data, including special category data, to be included in the bid request.

"*[...] Extended identifiers support in the OpenRTB specification allows buyers to use audience data in real-time bidding [...].*"



Object: Extended Identifiers

Extended identifiers support in the OpenRTB specification allows buyers to use audience data in real-time bidding. The exchange should ensure that business agreements allow for the sending of this data. Note, it is assumed that exchanges and DSPs will collaborate with the appropriate regulatory agencies and ID vendor(s) to ensure compliance.

Attribute	Type	Definition
`source`	string	Source or technology provider responsible for the set of included IDs. Expressed as a top-level domain.
`uids`	object array	Array of extended ID UID objects from the given `source`. Refer to Object: Extended Identifier UIDs.
`ext`	object	Optional vendor-specific extensions.

Offer of Proof: Partial printout of 1st defendant's Protocol Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object--extended-identifiers-, last accessed 03/24/2021,

submitted as **Annex K 103**

This can be used to send further unknown personal data, such as data from existing customer databases.

e) Sensitive data of the plaintiff were processed.

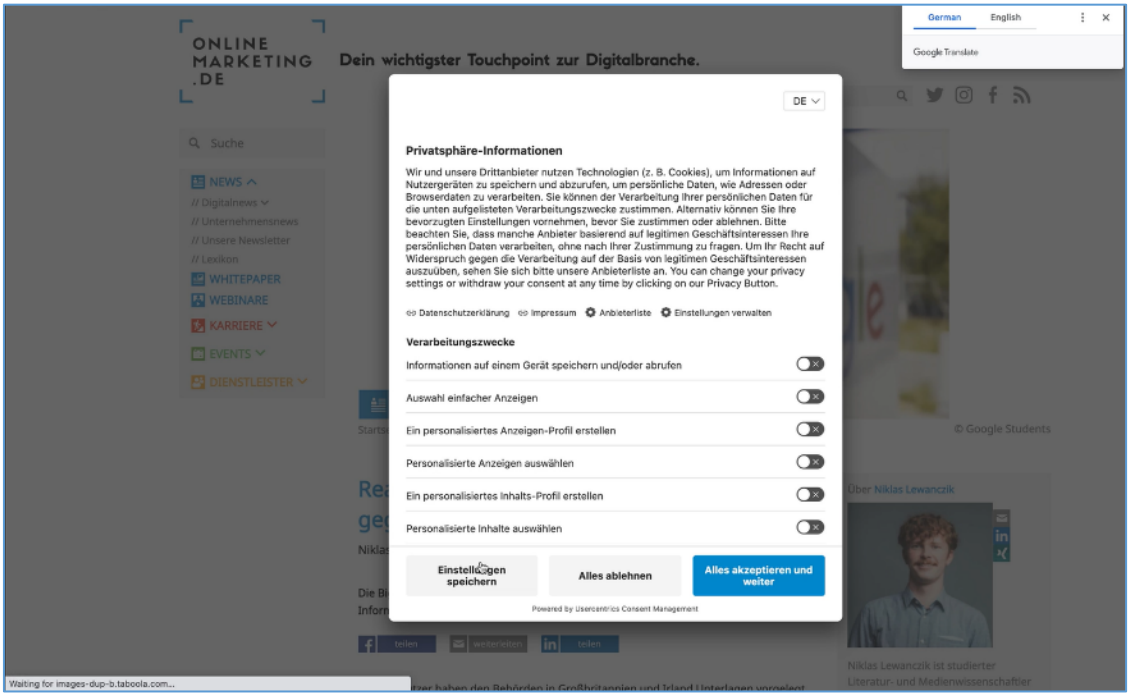
Plaintiff visited the website at the URL: https://onlinemarketing.de/karriere/unternehmenskultur/gefahrdet-mein-job-meine-gesundheit-corona-ruckenschmerzen-stress-risikofaktoren-arbeitsplatz and accessed an article there entitled "Is my job putting my health at risk? Corona, back pain and stress as risk factors in the workplace".

The fact that the plaintiff has called up this article allows conclusions to be drawn about his state of health, namely that he might be affected by stress or back pain or fear an infection with the coronavirus at his workplace. Regardless of whether categories according to the Content Taxonomy were transferred in the corresponding bid requests, these conclusions are already possible on the basis of the retrieved URL.

This information was sent to a large number of companies, as described in section A. II. 3. b) (p.49).

3. No request for explicit consent for special categories of personal data

When calling up the website of the 3rd defendant, no explicit consent is requested for the processing of the aforementioned special categories of personal data in accordance with art. 9 para. 2 lit. a GDPR.



Offer of Proof: Printout of the home page of the website at the URL www.onlinemarketing.de of the 3rd defendant dated 26/03/2021,

already submitted as **Annex K 26**

Offer of Proof: Entire Printout 3rd defendant's website, Privacy Information, as of 03/25/2021, available at: https://onlinemarketing.de, last accessed 03/25/2021,

submitted as **Annex K 104**

4. Contributions by the defendants

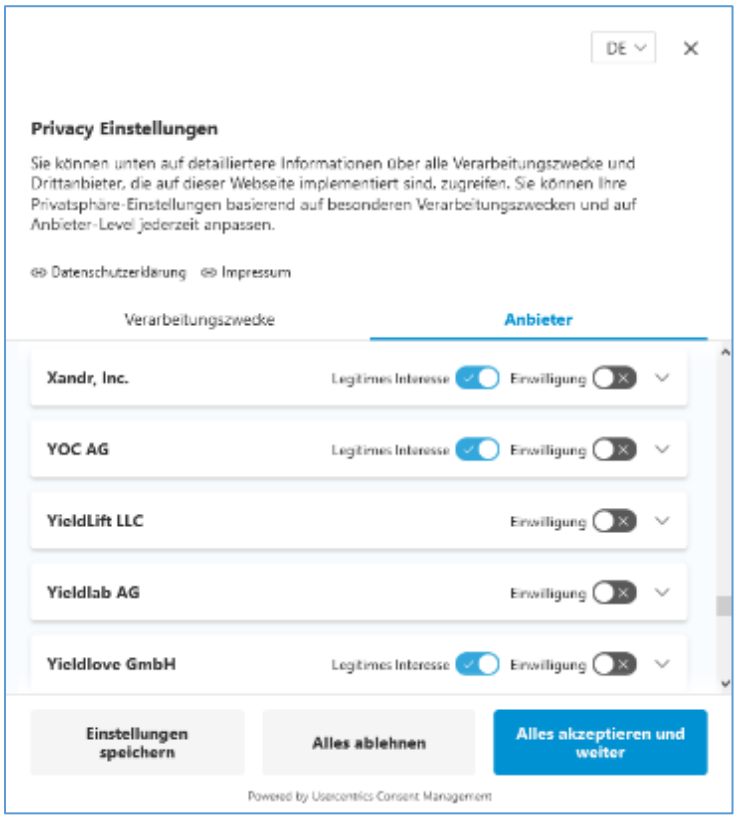
With regard to the contributions of the defendant, reference is made to the motion to 1 (point A. II.

5., p. 80).

V. Concerning motion 4

1. Transfer of data to third countries

The 3rd defendant states in the privacy settings on its website that it transmits personal data of website visitors, i.e. data of the plaintiff (section A. II. 3., p. 27f.) to the 2nd defendant in the USA on the basis of the technical standards provided by the 1st defendant (section A. II. 2., p. 25f.).



Offer of Proof: Partial Printout of 3rd defendant's website, Privacy Settings, as of 3/24/2021, available at https://onlinemarketing.de, last accessed 3/24/2021,

submitted as **Annex K 105**

The list of third parties to which personal data are transferred is more than 200 pages long. Data subjects must therefore scroll through 200 pages to understand the consequence of their consent.

Offer of Proof: Entire Printout of 3rd defendant's website, Privacy Settings, as of 03/25/2021, available at https://onlinemarketing.de, last accessed 03/25/2021,

submitted as **Annex K 106**

Neither in the data protection information nor in the privacy settings of the 3rd defendant is there any information on the existence of a so-called adequacy decision of the EU Commission, or any other appropriate or adequate guarantee to ensure an adequate level of protection, for the third country transfer to the USA [cf. complete printout of the data protection information of the 3rd defendant's website of 22.03.2021, available at https://onlinemarketing.de/datenschutzerklaerungen, last accessed on 22.03.2021, already submitted as **Annex K 2**].

Data transfers abroad in the context of real-time bidding auctions are also worrying US lawmakers. At the beginning of April this year, a bipartisan group of members of the US Senate sent a letter to the largest online advertising exchanges, including the American telecommunications company AT&T, of which the 2nd defendant is a subsidiary. In particular, the senators demand information on the foreign companies to which personal data is transferred during real-time bidding in order to be able to assess the resulting threats to national security [Patience Haggin, U.S. Senators Ask Digital-Ad Auctioneers to Name Foreign Clients Amid National-Security Concerns, Wall Street Journal Online, 02.04.2021 available at: https://www.wsj.com/articles/u-s-senators-ask-digital-ad-auctioneers-to-name-foreign-clients-amid-national-security-concerns-11617393964, retrieved on 06.04.2021].

2. Contributions by the defendants

With regard to the defendant's contributions, reference is made to the motion under 1 (point A. II. 5., p. 80f.).

B. Legal assessment

I. Admissibility of the action

1. International jurisdiction of the Hamburg Regional Court

The court seized has international jurisdiction pursuant to art. 79 para. 2 sentence 1 GDPR. For the establishment of international jurisdiction in disputes concerning claims arising from the GDPR, the existence of an establishment in Germany is sufficient.

The term "establishment" in art. 79 para. 2 sentence 1 GDPR is to be understood broadly. According to recital 22 p. 2 of the GDPR, establishment only requires "[...] the effective and real exercise of activity through stable arrangements." Furthermore, the third sentence of the recital states that "[t]he legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. "

For example, in the "Weltimmo" case, the ECJ ruled that the activities of an agency that operates a website and undertakes marketing activities are sufficient for the existence of an establishment by means of a "fixed establishment" [ECJ, judgment of 01.10.2015 - C- 230/14 = ZD 2015, 580, paras 28, 32 - Weltimmo].

Similarly, according to the judgment of the ECJ in the case "Google Spain and Google" on the concept of establishment under data protection law, the phrase "processing in the context of the activities of an establishment" must be interpreted broadly and effectively with a view to the protection of fundamental rights and freedoms (art. 7 and art. 8 CFR) [*ECJ*, Judgment of. 13.05.2014 - C-131/12 = ZD 2014, 350, para. 53 - Google Spain and Google]. In this respect, too, only advertising activities of an agency are sufficient. The decision states with regard to the activities of an establishment (para. 55):

> *"[...]if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.. [...]"*

Three specially seconded employees ("dedicated staff") and a managing director who acts as the public representative, permanently represent the 1st defendant in the business premises of vonwersch Digital Strategies GmbH in Hamburg, and handle key aspects of the 1st defendant's business and look after the market relations with partners in Europe, show that there is an effective

and actual exercise of an activity through stable arrangements. This establishment is recognizably of a permanent nature.

The 2nd defendant is permanently represented by the German subsidiary, AppNexus Germany GmbH, at its registered office in Hamburg.

The 3rd defendant is itself domiciled in Hamburg.

2. Local and subject-matter jurisdiction of the Hamburg Regional Court

The subject-matter jurisdiction of the Hamburg Regional Court follows from section 44 para. 1 sentence 1 of the Bundesdatenschutzgesetz (BDSG, Federal Data Protection Law) as the place of establishment of the controller.

Notwithstanding the foregoing, territorial jurisdiction is derived from section 32 ZPO, since the defendant's unlawful data processing constitutes a tortious act under national law.

Pursuant to sections 71 para. 1, 23 no. 1 Gerichtsverfassungsgesetz (GVG, Court Constitution Act), the court seized has subject-matter jurisdiction.

II. Merits of the action

The action is well founded.

1. Burden of proof of the defendant

The defendants have the full burden of proof for the lawfulness of the processing due to the legal regulation. The established obligations to provide evidence from art. 5 and art. 24 GDPR also regulate the burden of proof.

The responsible parties are subject to a reversal of the burden of proof in data protection [*Kramer* in: *Paschke/Berlit/Meyer/Kröner*, Hamburger Kommentar Gesamtes Medienrecht, 2021, 9.1.76.C.IX., marginal no. 47].

If the controller cannot prove compliance with the principles of art. 5 para. 1 of the GDPR, contrary

to his accountability obligation under art. 5 para. 2 of the GDPR, this is at his expense [see *Herbst* in: Kühling/Buchner, DSGVO/BDSG, 2nd ed. art. 5, para. 77 et seq.]

Art. 24 para. 1 sentence 1 of the GDPR also contains an obligation to provide evidence, which, as part of an effective compliance and control system including the accountability obligation, also extends to the technical-organisational measures and precautions mentioned in art. 24 para. 1 of the GDPR, and is thus to be understood more broadly than the principles mentioned in art. 5 of the GDPR [*Hartung* in: Kühling/Buchner/DSGVO/BDSG, 2nd ed. 2018, art. 24, para. 20].

As a consequence of these obligations to provide evidence, the controller must always be able to prove that the processing is carried out in accordance with the requirements of the GDPR [*Hartung* in: Kühling/Buchner/DSGVO/BDSG, 2nd ed. 2018, art. 24, marginal no. 20]. Therefore, the obligations to provide evidence under art. 5 para. 2 GDPR lead to a reversal of the burden of proof in civil proceedings [cf. *Voigt*, in: v. d. Busche/Voigt, Konzerndatenschutz, 2nd ed. 2019, Part 2, Ch. 3, marginal no. 9 with further references].

Following this, also the LG Rostock [Urt. v. 15.09.2020 - Az.: 3 O762/19 = GRUR-RS 2020, 32027, Rn. 44 f.] has stated that the burden of proof for the lawfulness of the use of tracking technologies on websites is incumbent on the responsible party due to the general obligations of proof and accountability from art. 24 para. 1 GDPR and art. 5 para. 2 GDPR:

> *["The plaintiff has further argued, naming various tracking cookies, that there is a cross-website transmission of personal data, such as the IP address. With regard to the implemented tool "Google Analytics", the defendant has denied that it forwards the IP address to the third-party provider. In all other respects, however, it has* ***merely flatly denied that*** *a* ***cross-website*** *data transmission takes place.*
>
> *This is insufficient in this respect, as the* ***defendant*** *bears the* ***burden of presentation and proof that*** *the design of the* ***website complies with data protection law****, as follows from* ***art. 5(2) and art. 24(1) GDPR*** *(cf. BeckOK DatenschutzR/Schantz, 32nd ed. 1.5.2020, DS-GVO art. 5, marginal no. 39 with further references). Since the tracking technologies specifically named by the plaintiff (cf. pleading of 04.06.2020, p. 7) are not only in principle capable, but are also regularly used precisely for the purpose of collecting personal data and transmitting it to third-party providers, the defendant would therefore have to specifically plead and demonstrate that the aforementioned cookies do not transmit any personal data to other websites. It has not met this burden of presentation and proof. […]"*
>
> Emphasis by the author.

2. Joint data protection responsibility of the defendants

The defendants are jointly responsible for the processing of personal data of the plaintiff, in the sense of art. 4 para. 7 and art. 26 para. 1 sentence 1 GDPR. This processing was triggered by loading the website https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten,.

According to art. 4 No. 7 GDPR, a "controller" is 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. If two or more controllers jointly determine the purposes and means of the processing, they are joint controllers under art. 26 para.1, first sentence, GDPR.

a) Broad interpretation of the concept of liability

According to the established case law of the ECJ, the concept of controllership must be interpreted broadly. Both according to the wording and the objective [cf. art. 1 para.1 GDPR], a broad interpretation is necessary in order to comprehensively ensure the protection of the fundamental rights and freedoms of the data subjects (art. 7 and art. 8 CFR) [ECJ, Judg. v. 13.05.2014 - C-131/12 = ZD 2014, 350, para. 34 - Google Spain and Google; ECJ, judgment 05.06.2018 - C-210/16 = EuZW 2018, 534, para. 28 - Wirtschaftsakademie; ECJ, judgment v. 10.7.2018 - C-25/17 = ZD 2018, 469, para. 66 - Jehovah's Witnesses; ECJ, Judgment of. 24.09.2019 - C-136/17 = NJW 2019, 3503, para. 37 - Google/CNIL; ECJ, Judgment of. 29.7.2019 - C-40/17 = MMR 2019, 579, para. 66 - Fashion ID].

For the decision-making power over the purposes and means of data processing, it is not necessary that the controller itself is involved in the implementation of the processing [*Klabunde* in: Ehmann/Selmayr, DSGVO, art. 4 para. 36].

> *" Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties." [ECJ (Grand Chamber), Judgment of 13.5.2014 - C-131/12 para 34].*

The Article 29 Working Party has already confirmed in 2010 that data protection accountability may result from the actual influence on processing operations, especially in "*[...]complicated environments, often making use of new information technologies, where relevant actors are often inclined to see themselves as "facilitators" and not as responsible controllers."* [*Article 29 Working*

Party, WP 169, Opinion 1/2010 on the notions of "controller" and "processor", p. 14].

The determining factor for the decision-making power on the purposes and means of processing is therefore either

- an explicit legal competence in the form of a statutory regulation,
- an indirect responsibility based on current legal practice or traditional roles (e.g. employer), or
- the actual influence on the processing operation

[Article 29 Working Party, WP 169, Opinion 1/2010 on the notions of "controller" and "processor", pp. 12, 15 et seq; *Gierschmann*, ZD 2020, 69, 70].

The actual influence leads to the affirmation of a data protection responsibility. A formal assessment, e.g. how a contract is headed, is not relevant [*Article 29 Working Party,* WP 169, Opinion 1/2010 on the terms "controller" and "processor", p. 11 f.; *Laue/Kremer/Nink*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 1 marginal no. 52].

It is not necessary, according to the ECJ [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469 para. 69], that every controller has access to the data:

> *"[...] the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned[...]".*

b) Liability of the defendant

The joint responsibility of the defendants is a consequence of the joint decision on the purposes and means of the processing within the meaning of art. 26 para.1, first sentence, of the GDPR.

One of the purposes of the rules on joint responsibility is to protect the rights and freedoms of data subjects by ensuring that data subjects (e.g. website visitors or app users) can see a clear allocation of responsibilities. Otherwise, data subjects will not be able to exercise their rights under Art. 12-22 GDPR to the appropriate extent.

According to *Martini* [*Martini*, in: Paal/Pauly, DSGVO/BDSG, 2021, Art. 26 marginal no. 8], art. 26 GDPR is intended to take account in particular of hybrid forms of cooperation in the digital world, which generate new, collaborative accountability structures and thus make it more difficult for

data subjects *"to identify and understand whether personal data relating to them are being collected, by whom and for what purpose"* [cf. recital 58 p. 3 GDPR].

The provision aims to create clear attribution rules that counteract the incentive of a diffusion of responsibility.

This is confirmed by recital 79 of the GDPR:

> *"The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller."*

Petri [Petri in: *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht, Art. 26 DSGVO Rn. 2] directs the attention to the attribution criterion of the increase in risk through division of labour:

> *["Article 26 responds to the increasingly networked processing of personal data, which is characteristic of digitalisation and the Internet. If several or more entities process personal data cooperatively, this can have considerable data protection implications for the data subject: Services that cooperate in this way are not transparent for the users concerned, because and to the extent that they are unlikely to be able to understand the data flows that affect them. Processing of personal data based on the cooperation of several entities tends to increase risks; in particular, it can obscure who is actually responsible for a processing operation, who is thus the addressee of rights and obligations, and who may be liable in the event of damage. [...]"*

The processing guidelines of OpenRTB, AdCOM, Audience Taxonomy and Content Taxonomy of the 1st defendant define how Real Time Bidding operates. They specify what personal data are sent to thousands of companies to programmatically target individualized advertising, the way in which the data are transmitted to which actors, and which technical systems are used by the participants in this system.

aa) Criteria of the ECJ case law on actual influence on the purposes and means of processing

(1) In the **Jehovah's Witnesses case,** the ECJ had to deal with the joint responsibility of the Jehovah's Witnesses Community with its members with regard to the taking of notes for missionary and preaching purposes during home visits. The notes were not centrally recorded and their preparation was not prescribed by the Community.

The ECJ affirmed a joint responsibility according to the previous definition of controller with the same wording pursuant to art. 2 lit. d) of the Data Protection Directive (now art. 4 No. 7 GDPR). It ruled that the organization, coordination, and encouragement of promotional activity by the Community made it a data controller. [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 70, 75]. The GDPR definition of controller in art. 4 No. 7 is identical. Thus, the ECJ's reasoning applies also under the GDPR [GA Bobek, Opinion of 19.12.2018 - C-40/17, para. 87 - Fashion ID; *Schulz*, MMR 2018, 421, 422; *Gierschmann*, ZD 2020, 69, 70].

The relevant consideration for the assumption of joint liability was that one exerts influence over the Members "for his own purposes". The community did so, organising, coordinating and encouraging the processing of personal data [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 68 - Jehovah's Witnesses].

The ECJ ruled that the Jehovah's Witness Community was a data controller because it provided guidance on data collection, produced maps and made records of its members (who directly collected data from individuals) [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para 71]. There was no interaction of the community with the data subjects.

> *["Furthermore, not only does the Jehovah's Witnesses Community have knowledge on a general level of the fact that such processing is carried out in order to spread its faith, but that community organises and coordinates the preaching activities of its members, in particular, by allocating areas of activity between the various members who engage in preaching. [...]"*

Even the complete freedom of members to determine how and to what extent they process data in detail does not exempt the Community from a common attribution of processing [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 70 - Jehovah's Witnesses].

For the question of joint controllership, it is irrelevant whether each actor has equivalent responsibility [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 69 - Jehovah's Witnesses]. It is also irrelevant whether each controller has access to the data [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 69 - Jehovah's Witnesses].

Rather, controllership depends on the interests of the parties involved, and the influence they exert. According to the ECJ [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 69 - Jehovah's Witnesses]:

> *"[...] a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and*

who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46.[...]".

It was not necessary for the decision on the purposes and means of the processing to be by means of written instruction, or for collection of personal data to be mandatory [ECJ, judgment of 10.7.2018 - C-25/17 = ZD 2018, 469, para. 67 - Jehovah's Witnesses].

This can be directly applied to the activities of the 1st defendant: it provides guidelines and digital maps. The other actors, in particular the 2nd defendant, are members of the 1st defendant. The 1st defendant is also aware that processing operations of this kind take place, as it actively promotes them and benefits economically from these processing operations.

(2) The ECJ has ruled in the **"Wirtschaftsakademie" case** - still using the definition of controller in art. 2 lit. d of the Data Protection Directive - that the operator of a Facebook fan page is a joint controller with Facebook Ireland Ltd. for the processing of personal data of visitors to its page [ECJ, judgment 05.06.2018 - C-210/16 = EuZW 2018, 534, para. 44 - Wirtschaftsakademie].

An entity that operates a Facebook fan page determines the purposes of and the means for processing together with Facebook. This results from the actual processes during the use of the social network. A Facebook fan page can be created with a few "clicks" via Facebook's platform. Only the name of the fan page and optionally a description (e.g. company in Hamburg) have to be provided. After entering the contact details, a profile picture and a background picture can be selected and the page is ready. Subsequently, data about users' visits to the website as well as their activity are collected by Facebook and used by Facebook for evaluations. The behavior of visitors to the fan page is recorded on the basis of Facebook's technical specifications.

An operator of a fan page can ask for demographic data and statistics relating to its target audience(so-called insights). This entails Facebook processing these data, which the ECJ ruled made both the Operator and Facebook joint controllers [ECJ, Judgment 05.06.2018 - C-210/16 = EuZW 2018, 534, para. 37 - Wirtschaftsakademie].

Joint controllership arises from the tracking of user behavior by Facebook, as is also the case with Real Time Bidding. In this context, the operator of a Facebook fan page is involved in the decision on the purposes and means of the processing of personal data of the visitors of a Facebook fan page because of the parameterization carried out - inter alia, corresponding alignment with the target audience , and objectives of promoting its activities [ECJ, Judgment 05.06.2018 - C-210/16 = EuZW

2018, 534, para. 39 - Wirtschaftsakademie].

Specifically, the Court clarified that there did not need to be an equivalent responsibility, nor did each of the parties need to have access to the data. [ECJ, Judgment 05.06.2018 - C-210/16 = EuZW 2018, 534, para. 38 - Wirtschaftsakademie].

The final decision in the "Wirtschaftsakademie" case confirmed joint controllership with regard to tracking with cookies and similar tracking technologies. Thus, the Federal Administrative Court on the joint controllership of Facebook and an operator of a fan page made the following assumption with regard to tracking by means of cookies in the judgment of 11.09.2019 [Ref.: 6 C 15.18 = NJW 2020, 414 et seq.]:

> "*[...] The ECJ relies significantly on the consideration that the operator of a fan page maintained on Facebook, by setting up such a page, enables Facebook to place cookies on the computer or any other device of the person who has visited his fan page, irrespective of whether that person has a Facebook account (ECJ, Judgment of 5 June 2018, loc. cit. para. 35). In doing so, the operator makes a significant contribution to the processing of personal data of the visitors of the fan page (ECJ, Judgment of 5 June 2018 loc. cit. para. 36).*
>
> *In addition, the anonymous visitor statistics compiled by Facebook from the data enable the operator in general to design its information offering in as targeted a manner as possible (ECJ, judgment of 5 June 2018, loc. cit., para. 37). For the affirmation of a responsibility under data protection law, it is not necessary that, in the case of joint controllership of several operators for the same processing, each has access to the personal data concerned (ECJ, Judgment of 5 June 2018 loc. cit. para. 38). [...]"*

Conclusion: The mere use of a third-party infrastructure - including that of the defendants 1, 2 or 3 - that enables the user's behaviour to be traced, establishes joint liability.

(3) Finally, in the **"Fashion ID" case,** the ECJ confirmed joint controllership with regard to implementations of third-party technical standards.

Due to the implementation of the Facebook social plugin (Facebook Like button) in its website, Fashion ID (online shop of Peek & Cloppenburg) had decisively influenced the collection and transmission of personal data, which would not take place without an integration of the Facebook plugin [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 77 f. - Fashion ID].

Facebook's provision of the plugin, and the website operator's incorporation of that plugin into the source code of the website, jointly determined the means of data processing (art. 4 No. 7 GDPR)[ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 77 - Fashion ID].

As regards the purposes of the processing, the ECJ clarified that joint controllership can exist

without identiy of purposes when mutual economic interests are tacitly pursued by the controllers [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 80 - Fashion ID]. In order to benefit from this economic advantage, the website operator consents, at least implicitly, to the disclosure by transmission (art. 4 No. 2 GDPR) [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 80 - Fashion ID].

Even if Facebook alone took the decision to process the data for other purposes, the processing operations would be to both parties' mutual economic advantage, as they are the counterpart for the benefits offered by website operators [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 80 - Fashion ID].

Whether the website or app operator can access the transmitted data or not does not prevent it from being a joint controller [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 69 - Fashion ID].

It follows from the decision that website operators are jointly responsible with Facebook for compliance with European data protection law if they embed Facebook's "Like button" in the source code of their website (as JavaScript or iFrame etc.), and this plugin then processes the personal data of visitors to those websites.

In other words: Anyone who actively takes action and, like the 3rd defendant, embeds the third-party code of the 2nd defendant on his website on the basis of the 1st defendant's technical standards, thereby enabling data processing of visitors to his website, is also jointly responsible with the provider of the technical standards.

(4) Finally, according to the ECJ, further liability under national law, e.g. national civil law, contract law or tort law, remains untouched. For the question of joint controllership, it does not matter whether the website or app operator has access to the transmitted data or not [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579, para. 74 - Fashion ID].

If claims for injunctive relief and damages for unlawful data processing as violations of personality rights are based on German tort law (Sections 823 et seq. Bürgerliches Gesetzbuch (BGB, German Civil Code)), its broad attribution rules for accomplices and participants apply and a website or app operator must also be liable beyond the mere transfer of data to Facebook or other third parties for their more extensive violations of rights (cf. point B. II. 3.).

In this respect, reference should be made to the judgment of the Landgericht Dresden (LG Dresden, District Court Dresden) on the joint liability of a website operator and Google for the use of the

technical standard Google Analytics from the general right of personality from January 2019 [LG Dresden, Urt. v. 11.01.2019 - 1a O 1582/18, available at: https://www.spiritlegal.com/files/userdata_spiritlegal-com/downloads/19-06-20-LG-Dresden-Google-Analytics-Urteil.pdf, last accessed on 11.02.2020); cf. on this *Hense*, DSB 2019, 204].

bb) Enabling, coordinating, promoting and facilitating as effective influence

Defendant 1 not only enables, but it coordinates, it organizes, and it intensifies the processing of plaintiff's personal data by the Participating Companies through the provision, integration, and monitoring of its technical standards OpenRTB, AdCOM, Audience Taxonomy, and Content Taxonomy.

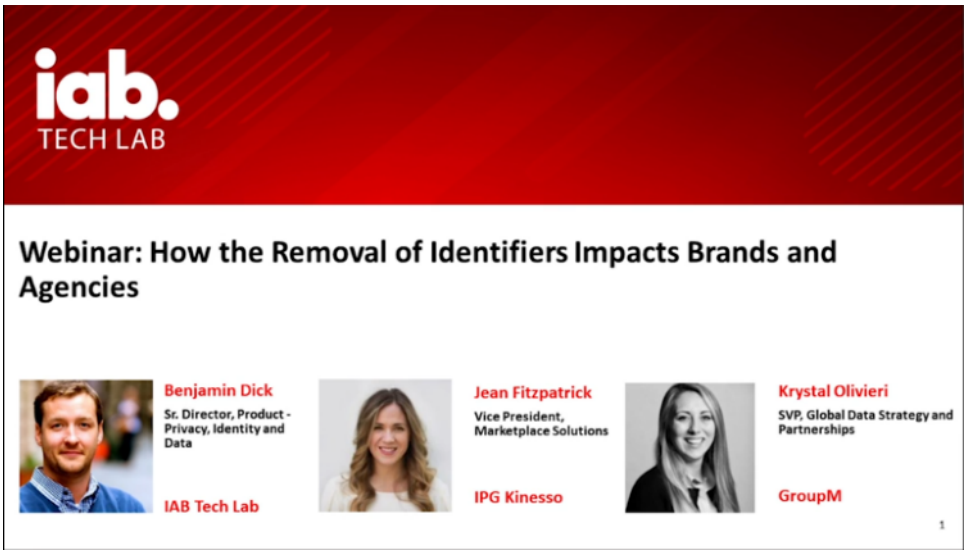
The 1st defendant specifies the types of personal data that can be disseminated and transmitted by means of a bid request and the rules according to which data are exchanged.

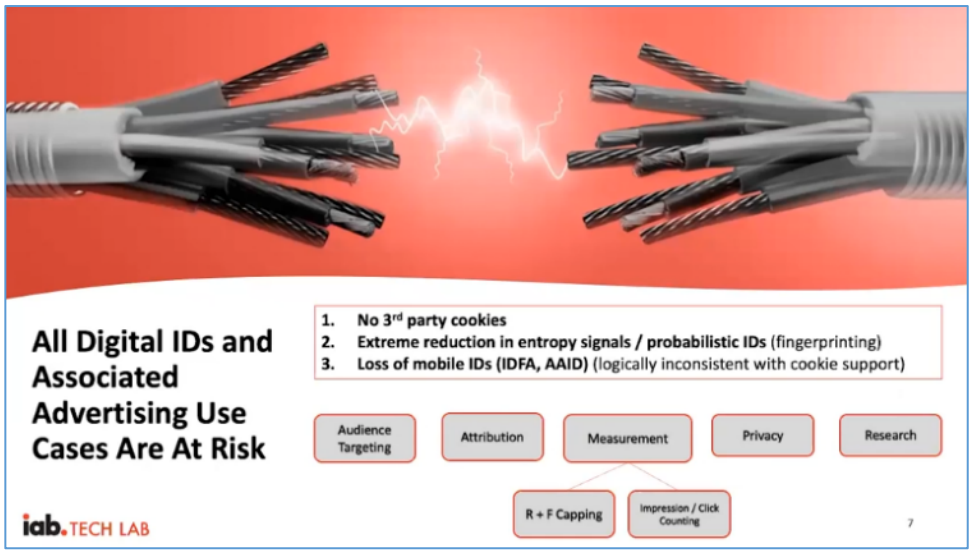
The technical protocols of the 1st defendant often encourage concrete processing operations, for example with formulations such as *"At least one of id or buyeruid is strongly recommended",* and facilitate the processing of data subjects' data through these concrete instructions for action (cf**. Annex K 24**).

Also, as part of defendant 1's training programs and through public statements, defendant 1 encourages and promotes companies to process personal data when conducting Real Time Bidding auctions.

The recording of defendant 1's webinar entitled "*How the removal of identifiers impacts agencies and advertisers,"* dated 07/21/2020 is available at: https://vimeo.com/442504076.

(Outlining the need for unique identifiers for defendant 1's standards to work in its 07/21/2020 webinar);





By providing tools to check whether the personal data in a bid request are processed correctly, the 1st defendant facilitates and enables the processing of the plaintiff's personal data at issue [see **Annex K 71**].

Influencing processing is also done for self-interest: As a subsidiary organization of the industry association International Advertising Bureau, Inc. (IAB), of which the 2nd defendant is a member, the 1st defendant represents the interests of the members of the association in the economic returns from Real Time Bidding, and related data trade.

The technical protocols of the 1st defendant that are the subject matter of the dispute provide far more extensive and detailed instruction on the aims and means of collecting personal data than the

brief guidelines on the questioning of persons by missionary members of the religious community of "Jehovah's Witnesses" in the ECJ decision.

Finally, the application of the criteria developed by the ECJ in the "Wirtschaftsakademie" decision also leads to the assignment of controllership of the defendants in the present case.

The most essential connecting factor for the Bundesverwaltungsgericht (BVerwG, Federal Administrative Court) in its final decision on the Facebook fan page [Urt. v. 11.09.2019 - 6 C 15.18 = NJW 2020, 414 et seq.] after the ECJ answered the questions referred is that the operator of a Facebook fan page sets the necessary condition for users to visit a certain Facebook page and that the operator of the fan page thereby makes the processing of personal data by Facebook possible in the first place.

The 1st defendant also sets the necessary conditions for data processing in the context of Real Time Bidding through its standards, their monitoring and curation, and is causally responsible for the associated processing of personal data. The extent to which it determines the processing operations exceeds the influence of a fan page operator in the aforementioned decision many times over.

cc) Joint decision on the means and purposes of processing

(1) The use of third-party technologies by website operators and other platform providers for analysis and advertising purposes corresponds to the circumstances clarified by the ECJ in the "Fashion ID" decision.

(2) Defendant 1 provides the technical standards OpenRTB, AdCOM, Audience Taxonomy and Content Taxonomy like a missionary guide to the data economy. Instead of believers, however, consumers are won over.

(3) Defendant 2 has set up its business model entirely around the implementation of these standards and the mass processing of personal data, thereby earning directly from the monetization of data subjects' privacy.

The contribution of the 2nd defendant in the context of the data processing in dispute (see already point A. II. 3., p. 27f.) is not only, in accordance with the "Wirtschaftsakademie" case [ECJ, Judt. 05.06.2018 - C-210/16 = EuZW 2018, 534] the mere provision of a platform as a central infrastructure where website operators such as the 3rd defendant can view guides on the

integration of Real Time Bidding - based on the 1st defendant's technical standards - and download programming codes for the implementation of the real-time auction of advertising spaces. Rather, the 2nd defendant provides detailed guidelines for the integration of programming codes for the implementation of real-time auctioning of advertising space based on the 1st defendant's technical standards for website operators [see **Annex K 75**], as does the 3rd defendant, and is therefore also jointly responsible under the standards of the "Jehovah's Witnesses" case.

In addition, defendant 2 explicitly provides programming code (API integration and JSON Fields) for publishers such as defendant 3 [**Annex K 76**].

(4) The 3rd defendant, in turn, uses its content to lure data subjects to its website in order to access their personal data there with the help of the 2nd defendant's technology, according to the exact specifications of the 1st defendant, and to auction it off to an unlimited number of third parties for commercial purposes.

As shown under point A. II. 3. (p. 27), the 3rd defendant has actively implemented programming code of the 2nd defendant in the source code of its website, which was developed on the basis of the 1st defendant's technical standards. As a result of the integration of defendant 2's programming codes, when defendant 3's website is accessed, multiple server requests are triggered to conduct Real Time Bidding auctions to defendant 2, as well as to other Advertising Exchanges. In line with the "Fashion ID" case [ECJ, judgment of 29.7.2019 - C-40/17 = MMR 2019, 579], the 3rd defendant is jointly responsible.

The 3rd defendant's server request transmitted, among other things, the user ID ("uuid2"), cookie information and information on the plaintiff's browser settings to the 2nd defendant. The server responses of the 2nd defendant about the results of the auction, using the technical standard "OpenRTB API Specifications Version 2.4" of the 1st defendant, then caused advertising material to be displayed on the 3rd defendant's website.

(5) Each defendant sets a condition that shapes the final outcome. Each defendant is causally responsible for the fact that the plaintiff's personal data is auctioned, because each defendant acts and earns in the auction process.

The actions of each defendant are each a piece of the puzzle without which the "marketing of users on websites" would not work. Only in the conscious and deliberate interaction of all defendants is

the demonstrated (unlawful) processing of the plaintiff's personal data possible.

Since the 1st defendant makes the processing of the user data possible in the first place through its standards, their implementation and distribution, it is involved in the decision on the purposes and means of the processing of the plaintiff's personal data, which, according to the case law of the ECJ, necessarily results in joint controllership within the meaning of art. 26 para. 1 sentence 1 of the GDPR with the other parties involved.

As regards the joint decision on the purposes of the processing, the ECJ clarified in the "Fashion ID" decision that mutually tacitly pursued convergent economic interests are sufficient. To enjoy its own economic benefits, the 1st defendant encourages the processing of the plaintiff's personal data by making its technical standards available, just like the ecclesiastical organizational structure of a missionary active religious community. The larger the number of members, the more prosperous the religious community. This consideration is also echoed by defendants: the more publishers, advertisers, and ad tech platforms submit to community standards, the more data can be processed and the greater revenue can be leveraged.

The integration of the technical standards of the 1st defendant into websites such as those of the 3rd defendant and into technology platforms such as those of the 2nd defendant enables the 1st defendant to optimize the advertising of products and thus to increase the sales of its own members. The facts of the case on this point of convergence of interests correspond almost entirely to those of the ECJ's "Fashion ID" decision.

For all defendants, the processing operations at issue secure mutual economic benefits. Defendant 1's OpenRTB technical standard generates annual sales of several billion euros in Europe alone.

3. Joint tortious liability of the defendants under section 830 BGB

(a) complicity of the defendants in the joint action

If one takes the German civil law conventions on co-perpetration as a basis [cf. *Wagner*, in: MünchKomm BGB, 2020, § 830 marginal no. 17], it must be stated that all defendants are jointly responsible as co-perpetrators in tort for the tortious acts committed by them.

The defendants, as links in a unified processing chain, unlawfully process plaintiff's personal data pursuant to a specific plan of action, with each defendant playing its part in enabling and allowing

the processing to succeed at subsequent stages.

The defendants bring about the unlawful processing through a conscious and deliberate cooperation based on a common plan of action. This plan of action is defined by the standard-setting organization 1st defendant in each individual point, so that a deviation from the plan of action manifested in the said standards is excluded. The contributions of each defendant are sine qua non for the success of the processing, and for the defendant's joint economic benefit, because all defendants share in the proceeds of the auction of the plaintiff's personal data.

The defendants are also aware of their complicity, because commercialization of the plaintiff's data is precisely the goal of the implementation of the 2nd defendant's technology and the standards of the 1st defendant on the 3rd defendant's website. Therefore, all defendants are aware of the circumstances of the action not only in broad outlines, but even in detail, and the defendants also have the respective will to carry out the action jointly with others or, in any case, to support it as another's action.

b) Incitement of the 1st defendant equates to complicity

Since accomplices, instigators and assistants are to be treated in the same way under tort law pursuant to section 830, Subsection 2, BGB, the legal distinction of the form of participation is irrelevant [cf. BGHZ 137, 89, 103 = NJW 1998, 377, 382 on the liability of demonstrators for damages for blocking a construction site for more than a short time - industrial park]. Even if for some reason one did not hold the 1st defendant complicit for its the elaboration and supervision of the plan of the action, as well as for the authority of the action, the 1st defendant is at least an instigator. The first defendant is liable as an instigator because it knowingly and willfully causes others to commit intentional tortious acts by its standards, and thereby fulfils the requirements of civil law instigation. Defendant 1 is aware that the standards it sets are used by defendants 2 and 3 in a manner that conforms to the standards, and which is therefore unlawful. The creation of situations that encourage the commission of an offence as a sufficient prerequisite for the act of instigation [see Bundesgerichtshof (BGH, Federal Court of Justice), judgement of 17.10.1979, ref.: 3 StR 401/79 = NStZ 1981, 69 ff] is the essence of the 1st defendant's mission.

According to the case law of the Federal Supreme Court, a communicative act between the instigator and the instigated is not required [*Wagner* in: *MünchKomm* BGB [2020], § 830 marginal no. 23]. Defendant 1 nevertheless communicates the illegal acts openly and unabashedly to all users of its standard and thus creates a pool of potential (co-)perpetrators in order to optimize the

financial gain of the acts. In this context, the 1st defendant does not even need to know the identity of those it instigates, because the intend of instigation encompass every implementer of its codified crime plan. If the target of the instigating act is elastic, the instigator's intent extends to the principal acts of each of the instigators.

c) Aiding and abetting by the 1st defendant equates to complicity

Aiding and abetting is also equivalent to complicity under tort law, section 830 para. 2 BGB. For the assumption of aiding and abetting, any form of assistance comes into consideration, including mere psychological support [BGH, judgment of 10.7.2012, ref.: VI ZR 341/10 = NJW 2012, 3439, 3441 marginal no. 15], whereby providing assistance in the preparatory stage is sufficient for establishing liability [BGH, judgment of 29.10.1974, ref.: VI ZR 182/73 = NJW 1975, 49, 52 on the joint liability of the psychologically supporting aider and abettor for assaults committed during demonstrations]. For the determination of an aiding and abetting act, the conscious promotion of another's act is sufficient [BGH, judgment of 22.2.2019, Ref: V ZR 244/17 = NJW 2019, 3638, 3642 marginal no. 46].

In a recent decision on the aiding and abetting liability of a foreign broker in the case of chanceless options businesses, the Federal Court of Justice (BGH) emphasized how immoral business models based on the division of labour also increase the risk of abuse for the parties concerned by expanding the circle of participants [BGH, judgement of 25.1.2011, ref.: XI ZR 195/08=NJW-RR 2011, 1193, 1195 marginal no. 33].

> *"...] Aiding and abetting within the meaning of section 830 BGB requires neither a communicative agreement between the principal offender and the aider and abettor on a common plan of action nor the participation of the aider and abettor in the execution of the act (cf. BGHZ 70, 277, 285 = NJW 1978, 816, 819). Rather, any conscious promotion of another's act is sufficient. If the broker in such a case, knowing of the high risk of abuse, has consciously and obviously opened the uncontrolled access to his online system to the intermediary without prior examination of his business model and at the same time has expressly permitted him to engage sub-brokers, he resigns himself to the realization of the recognized danger and thus approvingly accepts the damage to investors through an immoral business model practised in this context. The permission given by the broker to the intermediary to engage sub-intermediaries within the framework of his business model, which has remained uncontrolled, not only expands the circle of those involved, but also increases the danger of abuse known to the broker. [...]"*

The defendants work with technological assistance, due to the complexity in a division of labour, but always together, on the basis of a standardized plan of action to realize their business model, namely the real-time auctioning of personal data of data subjects. This business model is, as shown, contrary to applicable European and German data protection, privacy and tort law. The defendant's actions are so immoral that they even violate a whole series of prohibition laws as a targeted violation of legal requirements under Section 134 BGB (as lex specialis to Section 138 para. 1 BGB) [see OLG Frankfurt/Main, judgment of 24.1.2018, Ref.: 13 U 165/16 = NJW-RR 2018, 887 et seq. on the nullity of a contract for the acquisition of addresses].

> "*[...] It is recognized in case law and literature that a contract which obliges to commit unfair competition is null and void according to section§ 134 BGB [...]. However, the same applies to an address trading contract which violates section 28 III 1 BDSG because the consent of the data subjects required for a use of the data for purposes of address trading is missing. [...]"*

The regulations on the lawfulness of the processing of data in the GDPR constitute prohibition laws in the sense of section 134 BGB, since the regulations of art. 6 and 9 GDPR on the lawfulness of the processing of (special categories of) personal data are aimed at prohibiting transactions with these data due to their content, which necessarily involves an infringement of third party rights. The 1st defendant contributes to this business model by the standardization and training, in the supervising and assisting in the implementing of its unlawful standard, which enables, facilitates or intensifies the execution of the acts by the other accomplices and 2nd and 3rd defendants. Without defendant 1's preparatory work and assistance, defendants 2 and 3 would not be able to conduct the transactions described because they would not have a standard with which to do so. In every real-time auction and in every infringement of the rights of the affected persons caused thereby, the contributions of the 1st defendant are effective. Without it being necessary, the acts of the 1st defendant are a conditio sine qua non for the acts of the other joint tortfeasors and become effective in the joint tort. An offence cannot be committed even more jointly.

4. Merits of request 1

The plaintiff can demand that the defendants cease the processing of his personal data if it happens as under A. II. 3., p. 27f.

The claim arises from

- sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogue in conjunction with. art. 5 para. 1 lit. f, 24 para. 1, 32 para. 1, GDPR as well as from
- sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogue in conjunction with. art. 83 para. 4 lit. a) GDPR, section 41 para. 1 BDSG, art. 32 para. 1 GDPR.

a) Claim under sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with. art. 5 para. 1 lit. f, 24 para. 1, 32 para. 1 GDPR

(1) The contested data processing operations infringe art. 5 para. 1 lit. f, 24 para. 1, 32 para. 1 of the GDPR.

As shown, personal data is sent to thousands of companies through bid requests via defendant 1's technical standards through defendant 2 and defendant 3. The plaintiff has no way to protect his data against the unauthorized disclosure and processing in any way.

Art. 24 para. 1 sentence 1 of the GDPR requires data controllers to maintain technical and organisational measures to ensure compliance with the regulation and to provide evidence of such compliance:

> *" 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 organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.[...]"*

The design of the OpenRTB standard and the complementary standards creates possibilities for an extremely large number of actors to process extensive and intimate data about an even larger number of individuals. This is not matched by technical and organizational measures to effectively limit, for instance, the number of processors, the sets of data processed, the categories of data, or the purposes of processing.

The data protection principles of integrity and confidentiality pursuant to art. 5 para. 1 lit. f GDPR provide that personal data must be

> "*[...] processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by appropriate technical or organizational measures ('integrity and confidentiality'); [...]"*

The OpenRTB system, by its nature as a protocol for auctions as defined in the stakeholder specifications, is not able to guarantee the integrity and confidentiality of the data processed. OpenRTB does not provide any protection against unlawful or unauthorized processing of the data by thousands of companies receiving personal data through bidding requests.

Article 32 para. 2 of the GDPR:

> "*[...] In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. [...]"*

Adequate data security is part of the essence of the European fundamental right to "protection of personal data" as enshrined in article 8 of the Charter of Fundamental Rights [ECJ, Judgment of 8.4.2014, Joined Cases C 293/12 and C-594/12 - Digital Rights Ireland, para. 40; *Jarass* in: ibid. Charter of Fundamental Rights of the EU, 4th ed. 2021, art. 8, para. 15].

The European Court of Justice has consistently held, in relation to art. 8 of the CFR, that individuals whose personal data are affected by data processing operations must have sufficient guarantees from the controller to ensure effective protection of their data against risks of misuse [see most recently ECJ Judgment of 6.10.2020, Ref: C-623/17 - Privacy International, para. 68 with further references.].

What the defendants are engaging in is complete and warrantless user surveillance by technology and advertising companies on websites for the purpose of commercializing information about the population of the EU and the EEA. The collection of data on this scale is equivalent in its impact on fundamental rights to an unconditional data retention by the member states of the European Union, which can at least claim to fulfil the legislative mandate of effectively guaranteeing internal security.

However, even this data retention, which is one of the most controversial European legislative projects, has been set narrow limits by the ECJ, despite the benefits for the security of member states [ECJ, Judgment of 6.10.2020, Joined Cases Ref: C-511/18, C-512/18, C-520/18 - La Quadrature du Net and others, para. 138]:

> *["Moreover, such data retention must be subject to limitations and must be circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons concerned against the risk of abuse. Thus,*

that retention cannot be systematic in nature.. […]“

Safeguard mechanisms and guarantees are all the more necessary if, instead of internal security for the benefit of all citizens, only the commercial interests of a few companies are weighed in the balance of fundamental rights. The ECJ already provides for restrictions on state data collection to which access is only permissible in the event of "a serious threat to national security" [ECJ, [Grand Chamber], Judgment of 6.10.2020, Joined Cases Ref: C-511/18, C-512/18, C-520/18 - La Quadrature du Net and others, para. 139].

> *"[...] In view of the seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter resulting from a measure involving the general and indiscriminate retention of data, it must be ensured that recourse to such a measure is in fact limited to situations in which there is a serious threat to national security as referred to in paragraphs 135 and 136 of the present judgment.[...]."*

According to this jurisprudence, these and much stronger restrictions must apply a fortiori when data processing by private parties reduces rather than enhances the security of citizens.

The guarantee of European fundamental rights in Germany is ultimately incumbent on the Bundesverfassungsgericht (BVerfG, Federal Constitutional Court), also for disputes under private law [BVerfG, Order of 6.11.2019, Ref: 1 BvR 276/17 - Recht auf Vergessen II, Leitsatz 4 = NJW 2020, 314, 322, para. 96, 97].

(2) Due to the extremely high number of advertising recipients of a bid request and the sensitivity of the information transmitted, the processing operations entail very high risks for the data subjects and, in this case, the plaintiff.

The defendants have not taken appropriate technical and organizational measures to ensure a level of protection appropriate to the risk, in accordance with the "state of the art", as required by art. 32 para. 1 of the GDPR.

The state of the art in this sense is to be understood as a "developed stage of the technical possibilities at a certain point in time, based on appropriately secured knowledge of science, technology and experience" [DIN EN 45020:2007, term 1.4, Standardization and related activities - General terms].

For the proof of the "state of the art", the defendants are already burdened with proof according to

general rules, because the wording of the normative text in art. 32 GDPR as a preventive prohibition with reservation of permission imposes the burden of proof for compliance with the security of the processing on the controller. In addition, according to art. 5 para. 2 GDPR, the controller has the general burden of proof to demonstrate compliance with the data protection principles ("accountability"), which according to art. 5 para. 1 lit. f also includes data security.

The UK's data protection regulator, the ICO, in its report on Real Time Bidding [Information Commissioner's Office, Update report into adtech and real time bidding, 20.06.2019, available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, last accessed 10.02.2021, previously submitted as **Annex K 58, p. 21 f.**] 2019, found that also with regard to the OpenRTB technical standard, there are no safeguards or technical means of control for the processing operations of data subjects such as the applicant:

> *"[...] there are no guarantees or technical controls about the processing of personal data by other parties, eg retention, security etc.. In essence, once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls[...]".*

Without additional technical and organizational measures, including verification of the legal basis of the processing, data protection agreements with all (!) parties involved and regular documented audits, of which the defendants do not even fulfil one criterion, lawful processing is not possible:

> *["However, this contract-only approach does not satisfy the requirements of data protection legislation. Organizations cannot rely on standard terms and conditions by themselves, without undertaking appropriate monitoring and ensuring technical and organizational controls back up those terms. For example, ICO guidance on controller/processor and contracts and liabilities states that controllers must:*
>
> - *assess the processor is competent to process personal data in line with the GDPR;*
> - *put in place a contract or other legal act meeting the requirements in Article 28(3); and*
> - *ensure a processor's compliance on an ongoing basis, in order for the controller to comply with the accountability principle and demonstrate due diligence (such as audits and inspections)[...]" .*

The 1st defendant itself admitted in May 2018 that there are no technical and organizational measures in place to limit the use of personal data from bid requests [see **Annex K 12**]:

> "*[...] there is no technical way to limit the way data is used after the data is received by a vendor for decisioning/bidding on/after delivery of an ad [...]".*

However, if a measure does not (any longer) correspond to the state of the art, the controller violates its obligations if it fails to take the new measure and convert its system accordingly [*Mantz,* in: *Sydow*: Europäische Datenschutzgrundverordnung. 2nd edition 2018, art. 25 para. 38]. The defendants fail to take any technical-organizational measures at all to ensure data security, and in this way consistently violate all applicable legal requirements.

The information collected about the plaintiff's behavior through Real Time Bidding can lead to the creation of extensive profiles of the plaintiff's personality and life circumstances.

In the context of an auction, personal data can be sent out to thousands of companies via several advertising exchanges - according to the 2nd defendant. Also, each of the companies that receives the bid request can forward it to other companies. The high number of participants results in an equally high number of risks of unauthorized disclosure or unlawful processing. These risks of serious interference with fundamental rights, and their high probability of occurrence, are not matched by effective security measures.

Defendant 1's technical standards do not contain measures to control unauthorized disclosure or processing. The companies involved are not technically prevented, for example, from using information received for any conceivable purposes. Security of data processing, purpose limitation, transparency, data subject rights, deletion periods: all these are foreign words for the parties involved in the RTB auction system, including the defendants.

(4) Due to the fact that the defendants also process special categories of personal data, in particular health data of the plaintiff (cf. point B. II. 5. a), p. 152), the protective measures to be taken by the defendants are subject to particularly high requirements.

Verwaltungsgericht Mainz (VG Mainz, Administrative Court Mainz) recently put it aptly [VG Mainz, judgment of 17.12.2020, Az.: 1 K 778/19.MZ, in full text at BeckRS 2020, 41220, there Rn. 37]:

> *["It follows from all this that special protective measures must be taken in any case for data falling under Art. 9 or 10 of the GDPR, since in this respect a high risk must always be assumed on the basis of the general assessment under data protection law. [...]"*

The defendants do not have such special protective measures in place. Even the simplest safeguards are lacking. Inherent in the standards and technologies used is the insecure transmission to an uncontrollable multitude of recipients, because this allows defendants to conduct their auctions of online users' data without much technical effort.

The defendants must allow themselves to be accused of maintaining unlawful and insecure data processing and operating it intensively as a business model. In the case of the telecommunications company 1&1, the large criminal division of the Regional Court of Bonn found [LG Bonn, judgment of 11.11.2020, Ref.: 29 OWi 1/20 [final] = BeckRS 2020, 35663, para. 54]:

> "*[...] In a telecommunications company like the one concerned, the call centre is the primary point of contact for personal contact with the customer. It is therefore necessary to examine the level of data protection in the area of the call centre on an ad hoc basis and also at regular intervals. This already follows from the fact that data protection law is not static, but that the state of the art is also and especially evolving with regard to new risks. Accordingly, art. 32(1)(d) of the GDPR now also explicitly requires a regular review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing. The reform of the European data protection law through the introduction of the GDPR gave reason to review the data processing processes for compliance with the new law.*
>
> *K X did not use the transitional period for the introduction of the GDPR. In a corresponding review, the company would have had to make the same considerations as the Board. A similarly conscientious review based on the criteria of art. 32 GDPR would have led to the conclusion that the authentication process had to be improved. The necessary expertise for this existed on the part of K X. The company has its own legal department, as a telecommunications company it deals with data protection issues on a daily basis and must have special competences in this area. If doubts had remained, the BfDI would have been available as the competent supervisory authority to reliably clarify the questions of doubt. The infringement would have been avoided as a result. […]"*

A detailed examination of the legal situation, the evaluation of data security measures in the processing operation and the establishment of an adequate level of protection for the personal data of website visitors are the applicable legal requirements for the defendants. However, they have done nothing of the sort.

Defendant 1 consists of a conglomerate of technology companies, each of which has a legal department with appropriate expertise and the ability to obtain qualified outside legal advice.

The 2nd defendant is a subsidiary of WarnerMedia, a branch of the US telecommunications giant AT&T with an annual turnover of USD 171 billion (2020), and is undoubtedly equipped with the means to obtain adequate legal advice in every respect.

Even the 3rd defendant, as a leading industry portal, is in a position, due to its size and organizational structure, to adequately adjust to the applicable legal situation and to obtain external legal advice.

b) Claim under sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 83 para. 4 lit. a GDPR in conjunction with section 41 para. 1 BDSG

The claim also arises from sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with. art. 83 para. 4 lit. a GDPR in conjunction with section 41 para. 1 BDSG, because section 41 para. 1 BDSG is a protective law in the sense of section 823 para. 2 BGB, since the norms of the GDPR, to which the fine provision of section 41 para. 1 BDSG refers, protect data subjects' rights and freedoms. art. 32 para. 1 GDPR explicitly refers to the "risk to the rights and freedoms of natural persons", i.e. of any data subject. Since a violation of art. 32 GDPR is subject to a fine via art. 83 para. 4 a GDPR pursuant to section 41 para. 1 BDSG and this fine also serves the interest of the data subjects, the requirements of a protective law pursuant to section 823 para. 2 BGB are consequently met [see *Sprau* in: Palandt, BGB, 80th edition, 2021, section 823 no. 115].

5. Merits of request 2

The plaintiff can demand that the defendants cease processing his personal data if they do not provide him with the mandatory information under data protection law in a transparent and comprehensible and easily accessible form pursuant to art. 12 para. 1, 13 and 26 para. 2 sentence 2 of the GDPR, as set out in **Annex K 75.**

With regard to claim 2, the claim follows from sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 12 para. 1, art. 13 para. 1 and para. 2 GDPR as well as art. 26 para. 2 sentence 2 GDPR. In addition, the claim based on the transparency violation follows from sections 823 para. 1, 1004 para. 1 p. 2 analogous BGB in conjunction with. art. 2 para. 1 in conjunction with. art. 1 para. 2 Grundgesetz (GG, German Constitution).

a) Claim based on sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 12 para. 1, art. 13 para. 1 and para. 2 GDPR or art. 26 para. 2 sentence 2 GDPR

(1) Pursuant to art. 12 para. 1, first sentence, art. 13 para. 1 and art. 13 para. 2 of the GDPR, the defendants are obliged to provide the following information in a precise, transparent, intelligible and easily accessible form in plain and simple language cumulatively in relation to a specific

processing operation:

- the name and contact details of the person responsible and, where appropriate, of his representative;
- if applicable, the contact details of the data protection officer;
- the purposes for which the personal data are to be processed and the legal basis for the processing;
- where the processing is based on art. 6 para. 1 lit. f, the legitimate interests pursued by the controller or by a third party;
- where applicable, the recipients or categories of recipients of the personal data; and
- where applicable, the intention of the controller to transfer the personal data to a third country or an international organization and the existence or absence of an adequacy decision by the Commission or, in the case of transfers pursuant to art. 46 or art. 47 or the second subparagraph of art. 49 para. 1, a reference to the appropriate or adequate safeguards and how to obtain a copy of them or where they are available;
- the duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration;
- the existence of a right of access by the controller to the personal data concerned, as well as the right to rectification or erasure or to restriction of processing or a right to object to processing, as well as the right to data portability;
- where the processing is based on art. 6 para. 1 lit. a or art. 9 para. 2 lit. a, the existence of a right to withdraw consent at any time without affecting the lawfulness of the processing carried out on the basis of consent up to the moment of withdrawal;
- the existence of a right of appeal to a supervisory authority;
- whether the provision of the personal data is required by law or by contract or is necessary for the conclusion of a contract, whether the data subject is obliged to provide the personal data and what the possible consequences of not providing the personal data would be, and
- the existence of automated decision-making, including profiling, pursuant to art. 22 para.1 and para. 4 and, at least in those cases, meaningful information about the logic involved and the scope and intended effects of such processing for the data subject.

The data protection notices on the website https://onlinemarketing.de [cf**. Annex K 2**] of the 3rd defendant do not contain any information about the processing by the 2nd defendant nor any processing within the scope of the disputed technical standards of the 1st defendant for the real-

time auction of advertising spaces on the basis of the plaintiff's personal data (cf. point A. II. 3. a., p. 29f.). The failure to provide the legally required information constitutes a violation of art. 12 para. 1 sentence 1 of the GDPR (time, form and address) as well as article 13 para. 1 and para. 2 of the GDPR (lack of indication of purposes, legal bases, recipients, third country transfer, storage period and data subject rights).

(2) In addition, the defendants violated the specific information obligations under art. 26 para. 2 sentence 2 GDPR.

It has already been fully explained that the defendants jointly determine the purposes and means of the processing and therefore qualify as joint controllers (see point B. II. 2. b), p. 126).

Therefore, there is a joint responsibility according to art. 26 para. 1 sentence 1 GDPR, which is why, as a legal consequence, it must be specified in an agreement in a transparent manner which controller, i.e. which of the defendants, fulfils which obligations under the GDPR.

According to article 26 para. 2, second sentence, of the GDPR, the essence of the agreement must be made available to data subjects such as the plaintiff.

The purpose of these information requirements is, among other things, to protect the rights and freedoms of consumers by ensuring that a clear allocation of responsibilities is apparent to data subjects. Otherwise, data subjects will not be able to exercise their rights under art. 12 to 22 GDPR to the appropriate extent. This is confirmed by recital 79 of the GDPR:

> *"[...] The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. [...]"*

Information about the essence of joint controllership agreement for the processing at issue within the meaning of art. 26 para. 2 sentence 2 GDPR is not provided in the "Privacy Statement" [**Annex K2**] nor in the "Privacy Information" [**Annex 104**].

b) Claim under sections 823 para. 1, 1004 para. 1 sentence 2 BGB analogously in conjunction with. art. 2 para. 1 in conjunction with art. 1 para. 1 GG

Notwithstanding the above liability of the defendant, the plaintiff is entitled to injunctive relief under sections 823 para. 1, 1004 para. 1 sentence 2 BGB analogously in conjunction with. Art. 2 para. 1 in conjunction with art. 1 (1) GG due to the violation of the general right of personality.

The LG Dresden has affirmed a corresponding injunctive relief of a website visitor because the analysis service "Google Analytics" was implemented on the website and personal data such as the IP address and user ID were processed without a legal basis [LG Dresden, Urt. v. 11.01.2019 - 1a O 1582/18 = BeckRS 2019, 12930; Discussion: *Hense*, DSB 2019, 204 et seq.].

The scope of the processing of personal data in a bid request exceeds mere "analysis" of the usage behavior of a website many times over. This is all the more true when one considers that comprehensive movement profiles about the plaintiff can be created on the basis of the processed location data of the plaintiff.

The data processing impairs the plaintiff's general right of personality in the form of the right to informational self-determination pursuant to art. 2 para. 1 in conjunction with art. 1 para. 1 GG. It protects the individual against the unlimited collection and processing of his or her personal data in order to prevent resulting restrictions on his or her freedom of action [BVerfG, judgment of 13 April 1983 - 1 BvR 209/83 - Volkszählung = NJW 1984, 419 et seq.].

The right to informational self-determination must also be observed in the relationship between private parties due to indirect third-party effect and therefore has an impact on civil law as a constitutional value decision [BVerfG, Order of 6.11.2019 - 1 BvR 16/13 - Right to be Forgotten I, paras. 86, 87]. It includes here the possibility,

> *"[...] to exert a differentiated influence on the context in which and the manner in which one's own data are accessible to and used by others, and thus to have a substantial say in the attributions that apply to one's own person [...]".*

In particular, the right to informational self-determination between private parties grants protection against this [BVerfG, Order of 6.11.2019 - 1 BvR 16/13 - Recht auf Vergessen I, para. 90],

> *"[...] that third parties seize individual data and use them in an incomprehensible way as an instrument to determine the persons concerned to characteristics, types or profiles over which they have no influence and which are, however, of considerable importance for the free development of the personality as well as an equal participation in society. [...]"*

What the Federal Constitutional Court makes emphatically clear in this judgment with the words "in an incomprehensible manner" is a separate national transparency principle for complex automated data processing, which is already known from the "census judgment" [BVerfG, judgment of 13.04.1983 - 1 BvR 209/83 - census = NJW 1984, 419, 422].

> *"[...] Anyone who is not able to assess with sufficient certainty what information concerning him or her is known in certain areas of his or her social environment, and anyone who is not to some extent able to assess the knowledge of possible communication partners, can be substantially inhibited in his or her freedom to plan or decide on the basis of his or her own self-determination. The right to informational self-determination would not be compatible with a social order and a legal order enabling it in which citizens can no longer know who knows what, when and on what occasion about them. Those who are uncertain whether deviant behaviors will be noted at any time and permanently stored, used or passed on as information will try not to be conspicuous by such behaviors. [...]"*

For it is precisely this knowledge of the data-processing processes and their consequences that is the prerequisite for freedom of action, without which there can be no informational self-determination. The data subject must not only be informed about the purpose of the processing, he must know exactly "who knows what, when and on what occasion" about him [*Munz* in: Westphalen, Graf von/Thüsing, Vertragsrecht und AGB-Klauselwerke, Stand: 46. EL, 2020].

The individual is therefore to be protected not only from the disclosure of data which he does not wish to disclose, "but also of such data whose significance as a 'fact of life' he is not even in a position to assess" [*Kunig/Kämmerer* in: von Münch/Kunig, Grundgesetz (7th edition, 2021), art. 2 marginal no. 77]. And the defendants must also allow themselves to be confronted with these considerations, which are shaped by fundamental rights, in their capacity as private commercial enterprises, because in the scope of the right to informational self-determination between private parties, the power relationships of the parties involved must be taken into account. The more dominant the position of the responsible party, the closer the scope of the fundamental rights obligation is to that of the state [BVerfG, Order of 6.11.2019 - 1 BvR 16/13 - Right to be Forgotten I, para. 88].

Due to its immense market-dominating influence, the 1st defendant must allow itself to be measured against a particularly strict standard with regard to its commitment to fundamental rights [see Oberlandesgericht Dresden (OLG Dresden, Higher Regional Court Dresden), order of 07.04.2020 - TwitterSperrt I = BeckRS 2020, 7500; Az. 4 U 2805/19; OLG Nuremberg, decision of 06.04.2020, ref. 3 U 4566/19 - TwitterSperrt II; in each case with the participation of the plaintiff's legal representatives as well as OLG Nuremberg, judgment of 4.8.2020, ref.: 3 U 3641/19 -

Goldstücke].

The fact that the plaintiff visited the aforementioned websites and which media he consumed is relevant information from which his interests and personal traits can be derived and which can be assigned to the plaintiff's personal sphere. The data processing are significant encroachments on the right to informational self-determination due to the large number of advertising companies that received information about his visit (without his necessarily being aware), and due to the inevitable and routine profiling of the plaintiff, as well as the use of his personal data for advertising, commercial or even political purposes.

The 1st defendant exerts a determining influence over this data processing and advertising platforms by its industry standard, which is used by thousands of companies worldwide. It is almost impossible for data subjects to escape that influence in the everyday use of websites and apps.

The lack of transparency of the data processing, which is expressed in the breach of the legally standardised information obligations of the GDPR, also leads to an illegality of the processing at issue when applying purely national tort and constitutional law.

6. Merits of motion 3

The plaintiff can demand that the defendants refrain from processing his personal data if they do so as explained under A. IV. 1., p. 93et seq.

With respect to motion 3, the claim follows from:

- sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 9 para. 1, para. 2 GDPR,
- sections 823 para. 2, 1004 para. 1 p. 2 BGB analogue in conjunction with section 15 para. 3 Telemediengesetz (TMG, German Telemedia Act) in conjunction with art. 6 para. 1 p. 1 lit. a GDPR and from
- sections 823 2, 1004 para. 1 sentence 2 BGB analogue in conjunction with. art. 5 para. 1 lit. f, 32 para. 1 GDPR.

a) Claim based on sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 9 para. 1 and para. 2 GDPR

The very fact that plaintiff accessed an article titled: "Is my job putting my health at risk? Corona, back pain and stress as risk factors at work" allows conclusions to be drawn that the plaintiff is affected by the aforementioned health-related problems. Therefore, it is a special category data according to art. 9 para. 1 GDPR.

According to their own documentation, the defendants also use context-related information in the processing in question in accordance with the technical standards Context Taxonomy and Audience Taxonomy (see A. II. 3. a), p. 44IV. 2. b) bb) and cc), p. 105f.)).

The processing of such data is prohibited under art. 9 para. 1 of the GDPR unless one of the conditions set out in paragraph 2 applies. This is not the case. In particular, the plaintiff has not given express consent to the processing of such data, art. 9 para. 2 lit. a GDPR.

(1) According to the correct view of the UK supervisory authority (ICO) and the Irish supervisory authority, due to the assignment of a e.g. health-specific context - defined in content taxonomies of the IAB (e.g. Content Taxonomy v.2.0, available at: https://iabtechlab.com/blog/iab-tech-lab-announces-final-content-taxonomy-v2-ready-for-adoption/, last accessed on 08.02.2021) - the user data transmitted in a bid request are special categories of personal data (health-related data) within the meaning of art. 9(1) of the GDPR [see Information Commissioner's Office, Update report into adtech and real time bidding, already submitted as **Annex K 58,** p. 13].

The same applies if data subjects are classified into, for example, health-related segments by means of target group formation (e.g. "Audience Taxonomy v.1.1" of 12.02.2021, available at https://iabtechlab.com/standards/audience-taxonomy/, last accessed on 07.04.2021).

The practice has not changed to date. The ICO is still of the opinion that such information on website content regarding the content taxonomy within a bid request is to be regarded as special categories of personal data within the meaning of art. 9 para. 1GDPR [see the results of the consultation of the UK supervisory authority with industry representatives on bid requests: ICO Adtech Fact-Finding Forum of 19 November 2019, available at https://ico.org.uk/media/about-the-ico/documents/2616750/fff2-bid-requests-201912.pdf and https://ico.org.uk/media/about-the-ico/documents/2616754/fff2-info-gathering-201912.pdf, last accessed on 07.02.2021].

Similarly, the Irish Data Protection Commission classifies the attribution of content taxonomies to a user profile from contextual data based on the association with personal data of the user when visiting the website as health-related data within the meaning of art. 9 para. 1 GDPR by endorsing the view of the ICO [see Report by the Data Protection Commission on the use of cookies and other tracking technologies of 06.04.2020, p. 10 f., p. 18, available at: https://www.dataprotection.ie/sites/default/files/uploads/202004/Data%20Protection%20Commission%20cookies%20sweep%20REVISED%2015%20April%202020%20v.01.pdf, last accessed on 10.02.2021].

The Supreme Court of Austria (OGH) has recently ruled that the grouping of data subjects into marketing categories or the addition of categories to a person constitute personal data under art. 4 No. 1 GDPR: [OGH, Urt. v. 18.02.2021 - 6 Ob 127/20z, available at: https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20210218_OGH0002_0060OB00127_20Z0000_000/JJT_20210218_OGH0002_0060OB00127_20Z0000_000.pdf, last accessed on 07.04.2021]. In this context, the OGH stated with regard to marketing classifications by Österreichische Post AG:

> *"[...] In the sense of the opinion set out in 2.1, the information to be assessed here is subject to the regime of the GDPR, since it is directly associated with the plaintiff and contains statements about, for example, his preferences and attitudes; whether the assessments are actually accurate, on the other hand, is irrelevant [...]."*

If a classification is assigned to a person, then this constitutes a personal data in the sense of the GDPR. Thus, the Supreme Court explicitly classifies data stored for advertising purposes, e.g. when residents of a street are assigned to a certain buyer group or purchasing power class based on the population structure, as personal data [Supreme Court, judgment of 18.02.2021 - 6 Ob 127/20z, para. 17].

The Federal Administrative Court in Austria (BVwG) has ruled in this sense that marketing measures based on "[...] special categories of personal data in the context of the exercise of the trade of 'address publishers and direct marketing companies' [...]" are invalid under art. 9 para. 1 and para. 2 lit. a GDPR [BVwG, decision of 26.11.2020 - W258 2227269-1/14E, available at: https://www.bvwg.gv.at/presse/Datenschutzverfahren_Oesterreichische_Post.html, last accessed on 07.04.2021].

The Austrian Federal Administrative Court held that the linking of party affinity with an individual person fulfilled the content element of personal information; thus, even if the actual political opinion of the person concerned is not known, party affinity contains a direct statement about the

specific person, namely with what probability he or she is interested in advertising from a specific political party; this statement, even if it is subject to a statistical range of fluctuation due to the method of determination, is not entirely random, but is derived from correlations obtained from opinion polls and election results; it is a statistically based assessment of the person with regard to his or her interest in advertising for a particular political party [BVwG, decision of 26.11.2020 - W258 2227269-1/14E, para. 3.2.3].

In order to determine what are special categories of personal data, the Supreme Administrative Court of Austria stated:

> *["Due to the wording of art. 9 (1) GDPR, according to which the prohibition relates to the processing as such, it is only the fundamental suitability of the types of data to trigger these risks that is relevant. The specific processing context, such as the purpose of the processing or specific processing steps, are thus not to be taken into account in assessing whether a personal data item is to be classified under one of the special categories of data (disputed in the case of indirectly sensitive data; denying the context of use, e.g. Petri in Simitis/Hornug/Spiecker (eds.) Datenschutzrecht (2019) art. 9 Rz 12 with reference to Bergauer in Knyrim Das neue Datenschutzrecht in Österreich and probably also Schiff in Ehmann/Selmayr Datenschutz-Grundverordnung[2] Art 9 Rz 2 f; aA Schulz in Gola Art 9 Rz 13; Weichert in Kühling/Buchner (eds.), DSGVO[2] Art 9 Rz 22) [....]".*

(2) Each of the defendant's bid requests contain information on, among other things, the plaintiff's religion, political views, health and income can be processed as special categories of personal data within the meaning of art. 9 para. 1 of the GDPR. In the course of each individual (!) of server request shown (cf. point A. II. 3. a), p. 29et seq.), at least the complete IP address, information about the device and software, as well as the User ID is processed. For example, the User ID 6390846609290577797 was assigned to the plaintiff by the 2nd defendant when the plaintiff loaded the 3rd defendant's website. This information therefore also has a personal reference.

According to the case law of the ECJ [Judgment of 19.10.2016 - C-582/14, para. 48 - Breyer], the possibility of attribution to users' plain names or other direct identifiers is sufficient:

> *"[...] Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.[...]"*

Similarly, according to the highest court ruling of the Federal Court of Justice, a randomly generated number stored in cookies (user ID of the third-party provider) constitutes a pseudonym within the meaning of Section 15 para. 3 TMG. S. d. § 15 para. 3 TMG [BGH, Urt. v. 28.05.2020 - I ZR 7/16 -

Cookie Einwilligung II = MMR 2020, 609, 611; agreeing *Menke*, K&R 2020, 650, 652; *Baumgartner/Hansch*, ZD 2020, 435, 436], whereby the BGH still referred to the legal definition in section 3 para. 6a BDSG old version. Even pseudonymous data constitute personal data according to recital 26 p. 2 GDPR, and even pseudonymous data constitute personal data within the meaning of art. 4 No. 1 GDPR.

(3) On the website https://onlinemarketing.de of the 3rd defendant, there is no request for effective consent (for more details, see B. II. 5. b. p. 155f.) in accordance with art. 4 No. 11, art. 6 para. 1 lit. a and art. 7 GDPR for the processing in dispute.

(4) A fortiori, there is no explicit consent under art. 9 para. 2 lit. a GDPR for the processing of special categories of personal data such as health data. The defendant's Transparency & Consent Framework (1) itself states that it cannot cover the processing of special categories of data.

Similarly, no other justification under art. 9 para. 2 GDPR is relevant for the basic prohibition to process health-related data or other special categories of personal data.

b) Claim from sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogue in conjunction with. section 15 para. 3 TMG in conjunction with art. 6 para. 1 p. 1 lit. a GDPR

aa) Mandatory consent requirement for the processing at issue

The unlawfulness of the use of tracking technologies for the storage of information and access to information already stored in the terminal device without informed and voluntary consent of the user was confirmed by the BGH after the ECJ decision "Planet49" [Urt. v. 28.05.2020 - Ref: I ZR 7/16 - Cookie consent II = NJW 2020, 2540].

Contrary to the wording of the provision, the BGH interpreted Section 15 para. 3 TMG in accordance with art. 5 para. 3 of the ePrivacy Directive. Pursuant to art. 5 para. 3 sentence 1 ePrivacy Directive (Directive 2002/58/EC as amended by Directive 2009/136/EC), any storage of information and any access to information already stored in a user's terminal equipment requires the user's consent on the basis of clear and comprehensive information provided to the user.

Irrespective of this, the GDPR applies in addition to the provisions of the TMG, which must be interpreted in conformity with the Directive, insofar as corresponding technologies also process

personal data of the users, as is naturally the case with tracking technologies. Both regulations are based on entirely different protective purposes, as the BGH correctly observes in its decision that art. 5 para. 3 ePrivacy Directive does not concern the scope of application of the GDPR, as [BGH, judgment of 28 May 2020 - I ZR 7/16, para. 61 - Cookie Consent II].

However, the two regulations apply side by side where technologies requiring consent under art. 5 para. 3 ePrivacy Directive also process personal data, in view of the conflict of laws provision in art. 95 GDPR [*Gierschmann*, MMR 2020, 613 (614 et seq.); *Spittka*, DB 2019, 2850 (2854)]. However, this is of limited relevance in practice, as effective consent pursuant to art. 5 para. 3 ePrivacy Directive is usually also effective consent within the meaning of art. 6 para. 1 sentence 1 lit. a GDPR due to the reference for the definition of consent and the information requirements in the GDPR (previously Directive 95/46/EC and due to art. 94 para. 2 sentence 1 GDPR in the GDPR).

Since these refer to art. 5 para. 3 of the ePrivacy Directive via the interpretation of Section 15 para. 3 TMG in conformity with the Directive, and this in turn refers to the concept of consent in art. 4 No. 11 GDPR, various legal concepts of the GDPR apply in the present case.

Therefore, in the case of terminal access involving special categories of personal data within the meaning of art. 9 para. 1 of the GDPR, the requirements of art. 9 para. 2 lit. a of the GDPR apply.

Due to the access to and storage of personal data of the plaintiff during his visit to the website of the 3rd defendant by means of tracking technologies of the 2nd defendant on the basis of the technical specifications OpenRTB, AdCOM, Audience Taxonomy and Content Taxonomy of the 2nd defendant, consent is required pursuant to section 15 para. 3 sentence 1 TMG in conjunction with art. 5 para. 3 sentence 1 ePrivacy Directive. Consent is required in accordance with art. 4 No. 11, art. 6 para. 1 sentence 1 lit. a, art. 7 of the GDPR.

In addition to the judgment of the Rostock Regional Court [judgment of 15.09.2020 - ref.: 3 O762/19 = GRUR-RS 2020, 32027, marginal no. 44 f.], the Cologne Regional Court has now also explicitly assumed a violation of Section 15 para. 3 TMG if access to or storage of data on a user's terminal by means of cookies takes place without effective consent [judgment of 29.10.2020 - ref.: 31 O 194/20 = GRUR-RS, 2020, 37085].

Consequently, all processing of personal data of the plaintiff referred to, in particular such data in RTB bid requests, is subject to a consent requirement pursuant to Section 15 para. 3 TMG in

conformity with art. 5 para. 3 sentence 1 of the ePrivacy Directive.

With regard to the interpretation of section 15 para. 3 TMG and the Directive, the BGH has also assumed that the exception from the consent requirement under art. 5 para. 3 sentence 2 of the ePrivacy Directive must be taken into account [BGH, judgment of 28 May 2020 - I ZR 7/16, para. 49 - Cookie consent II].

> *"[...] In the case in dispute, the storage or retrieval of the information is not technically necessary within the meaning of the second sentence of art. 5(3) of Directive 2002/58/EC, but is for advertising purposes, so that the exception to the consent requirement does not apply. [...]"*

bb) Ineffective consent mechanism on the website of the defendant 3

Even if the plaintiff presses the button "Accept all and continue" on the first layer of the cookie banner displayed on the 3rd defendant's website [cf. partial printout of the "Privacy Information" of the 3rd defendant's website "www.onlinemarketing.de" of 25.03.2021, already submitted as **Annex K 26**], there is no effective consent.

The request for presumed consent is invalid for four reasons.

(1) Firstly, the purported consent is inadequate, pursuant to Section 15 para. 3 sentence 1 TMG in conjunction with art. 5 para. 3 sentence 1 ePrivacy Directive in conjunction with art. 4 No. 11 GDPR because of a lack of information.

According to art. 4 No. 11 GDPR, consent must be given "in an informed manner".

The Chief Executive of IAB Europe, Townsend Feehan, admitted a year before the publication of the Transparency & Consent Framework that it was technically impossible to request informed consent under the GDPR from users for the fully automated targeting of. The lobby association's letter to the EU Commission [already submitted as **Annex K 60**] urged that an exemption from the E-Privacy Regulation (not yet adopted) be created for OpenRTB, otherwise the online advertising business practice would no longer be viable.

> *"[...] it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario [...]".*

Prior information requirement will "break" programmatic trading

Consent under the GDPR must be "informed", that is, the user consenting to the processing must have *prior* information as to the identity of the data controller processing his or her personal data and the purposes of the processing.[5] As it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario, programmatic trading, the area of fastest growth in digital advertising spend, would seem, at least *prima facie*, to be incompatible with consent under GDPR – and, as noted above, if a future ePrivacy Regulation makes virtually all interactions with the Internet subject solely to the consent legal basis, and consent is unavailable, then there will be no legal be no basis for such processing to take place or for media to monetise their content in this way.

The ECJ confirmed in the "Planet49" case that the clear and comprehensive information for consent under art. 5 para. 3 sentence 1 of the ePrivacy Directive also includes information on the functional duration of the cookies and whether third parties have access to the cookies [ECJ, Judgment of 01.10.2019 - C-673/17 = EuZW 2019, 916, para 75 f.]. In detail, the Court stated:

> *"[...] In a situation such as that at issue in the main proceedings, in which, according to the file before the Court, cookies aim to collect information for advertising purposes relating to the products of partners of the organiser of the promotional lottery, the duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information which must be provided to the user in accordance with art. 5(3) of Directive 2002/58.*
>
> *76. In that regard, it should be made clear that Article 10 of Directive 95/46, to which art. 5(3) of Directive 2002/58 and art. 13 of Regulation 2016/679 refer, lists the information with which the controller must provide a data subject from whom data relating to himself are collected. [...]"*

According to the information provided by the 2nd defendant, 1,647 companies can receive a bid request from it [see printout of the list of affiliated third parties of the 2nd defendant dated 12.01.2021, already submitted as **Annex K 13].**

In relation to users such as the plaintiff, who call up the website of the 3rd defendant, only a fraction of these possible recipients of a bid request are mentioned in the "privacy information" with which an alleged consent is to be queried [cf. total printout of the "privacy information" of the website www.onlinemarketing.de of the 3rd defendant of 25.03.2021, already submitted as **Annex K 104**]. Complete information about the recipients is also hardly possible, since the number of companies to which data can be transmitted is actually unlimited. IAB Europe's admission that it is technically impossible to request informed consent shows that in the run-up to the actual data processing it is not known which companies, and from which third countries, may receive sensitive information about the plaintiff.

Moreover, there is no sufficient description of the processing of the plaintiff's personal data in real time bidding auctions in accordance with the purpose limitation principle (art. 5 para. 1 lit. b GDPR). Purposes such as "serving personalized advertisements" do not convey the global and comprehensive processing of sensitive information involved.

(2) Secondly, there is no consent for the “specific” processing in the meaning of art. 4 No. 11 GDPR.

In the case "Cookie Einwilligung II" [I ZR 7/16] decided by the BGH, the data subject had the possibility to select the advertising sponsors and cooperation partners from a linked list of 57 companies. If the data subject did not, then the defendant made the selection. The BGH declared that consent mechanism invalid because there was no consent for the specific case. In detail, the court stated:

> *["This is not the case in the dispute, because according to the findings of the appellate court, which are not objectionable under the law of review, the design of the declaration of consent challenged by the plaintiff is designed to confront the consumer with an elaborate procedure for deselecting partner companies on the list in order to induce him to refrain from exercising this choice and instead to leave the choice of advertising partners to the defendant. If the consumer, in the absence of knowledge of the content of the list and without exercising the right of choice, does not know which products or services of which entrepreneurs the consent covers, there is no consent for the specific case.*
>
> *The fact that the consumer may well recognize the given multiplicity of advertising partners, as the defendant's appeal asserts, does not alter the fact that the consumer will regularly have no knowledge of the concrete content of the consent given due to the design of the selection process. […]“*

The "provider list" linked on the first layer of the cookie banner of the 3rd defendant's website includes 676 third parties [cf. overall printout of the "privacy information" of the 3rd defendant's website www.onlinemarketing.de of 25.03.2021, already submitted as **Annex K 104**]. In this respect, a fortiori, there is no consent for the specific case.

(3) Thirdly, there is no unambiguous indication of consent within the meaning of art. 4 para. 11 GDPR if the only button provided is to accept all tracking-related data processing.

The Rostock Regional Court considered a comparable cookie banner with an "Allow cookies" button on the first layer that granted consent for around two dozen third-party companies, and concluded that in view of a button on the first layer on a cookie banner "Allow cookies", consent for data processing by means of cookies and similar tracking technologies was preselected and merely activated by pressing the button. The decision of the Rostock Regional Court [Urt. v.

15.09.2020 - Az.: 3 O762/19 = GRUR-RS 2020, 32027, Rn. 53] expressly states in this regard:

> *["An effective consent is therefore also not possible with the cookie banner now used. This is because all cookies are also preselected in this case and are "activated" by pressing the green "Allow cookie" button. Thus, the design of the cookie banner basically corresponds to the design in the case decided by the BGH.*
>
> ***It is true that** the **consumer has the option to have** the **details displayed** and to **deselect** individual **cookies. In fact, however,** the consumer **will** regularly **shy away from the effort of** such a procedure and **therefore press** the **button without prior information** about the **details**. In this way, however, the consumer does not know the consequences of his declaration. […]"*

The display of more than 100 listed affiliates in defendant 3's cookie banner discourages consumers from activating or opting out of certain tracking companies.

(4) Fourth, there is no unequivocal expression of will because the defendant has preselected consent. The defendant pre-selected consent for a number of tracking providers - including the 2nd defendant and Yieldlove GmbH, which is responsible for header bidding - in a misleading manner under the guise of a legitimate interest that does not exist in reality, i.e. it is already activated without a user having taken any action [cf. partial printout of the privacy settings on the 3rd defendant's website onlinemarketing.de dated 24 March 2021, already submitted as **Annex K 105**].

That buttons that have already been activated or ticked do not constitute an unequivocal declaration of intent is expressly stated in recital 32 of the GDPR and has been confirmed by the ECJ in the "Fashion ID" case (C-40/17).

cc) Blocking effect for the application of art. 6 para. 1 sentence 1 lit. f GDPR

As the extensive presentation of the facts has shown, a transmission of user data takes place due to the direct access to information in the user's terminal device - specifically at least the IP address and user ID in the user's browser.

Due to the direct access to terminal devices, section 15 para. 3 sentence 1 TMG in conjunction with art. 5 para. 3 ePrivacy Directive forbids the application of the legal basis in art. 6 para. 1 sentence

1 lit. f GDPR. The BGH decision "Cookie consent II" [judgment of 28.05.2020 - I ZR 7/16] confirms the priority of Section 15 para. 3 sentence 1 TMG in conjunction with art. 5 para. 3 ePrivacy Directive over legal bases of the GDPR:

> *"[...] art. 95 of the Regulation (EU) 2016/679 regulates the delimitation of the scopes of application of both legal acts in case of conflict, which is only given if both legal acts contain competing obligations pursuing the same objective. In this case, according to art. 95 of Regulation (EU) 2016/679, the provisions of the Directive take precedence (cf. Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 95 DSGVO Rn. 1, 17; Klabunde/Selmayr in Ehmann/Selmayr, DSGVO, 2nd ed., art. 95 Rn. 16). [...]"*

Therefore, the use of legitimate interest according to art. 6 para. 1 sentence 1 lit. f GDPR or other legal bases from art. 6 para. 1 GDPR is impossible.

c) Claim under sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 5 para. 1 lit. f, 32 para. 1 GDPR

Finally, the established case law of the ECJ confirms that the processing at issue infringes the data protection principles listed in art. 5 GDPR - cf. on the infringement of art. 5 para. 1 lit. f GDPR due to the lack of sufficient technical and organizational measures pursuant to art. 32 para. 2 GDPR already point B. II. 3. a), p. 140.

As the European Court of Justice has repeatedly ruled, in accordance with the provisions of Directive 95/46/EC:

> *"[...] any processing of personal data [...] must comply with the principles set out in art. 6 of the Directive as regards the quality of the data and with one of the principles set out in art. 7 of the Directive as regards the lawfulness of the processing of data" [ECJ, Judgment of. 29.07.2019 - C-40/17 marginal no. 93 = WRP 2019 1146 - Fashion ID; ECJ, judgment of 01.10.2015 - C-201/14, marginal no. 30 f. = ZD 2015, 577- Bara m. Anm. Petri; ECJ, judgment of. 20.05.2003 - C-465/00, C-138/01, C-139/01, para. 65 = EuR 2004, 276 - Österreichischer Rundfunk et al.; ECJ, Judgment of. 16.12.2008 - C-524/06, para. 48 = MMR 2009, 171 - Huber; ECJ, judgment of. 24.11.2011 - C-486/10, C-469/10, para. 26 = ZD 2012, 33 - ASNEF and FECEMD].*

It follows that the unlawfulness of the data processing required for the claim for injunctive relief under sections 823 para. 2, 1004 para. 1 sentence 2 BGB mutatis mutandis can result on the one hand from an infringement of the principles of data processing laid down in art. 6 of Directive 95/46/EC or art. 5 GDPR, and on the other hand from the non-existence of one of the conditions for the lawfulness of the processing in art. 7 of Directive 95/46/EC or art. 6 of the GDPR.

Because the GDPR's principles of processing and lawfulness of processing are identical, the case law of the ECJ remains valid under the GDPR.

7. Merits of motion 4

The basis of claim for motion 4 is sections 823 para. 2, 1004 para. 1 sentence 2 BGB analogously in conjunction with art. 45, 46 GDPR.

The defendants also transfer personal data of the plaintiff to the USA. In its judgment in Case C-311/18 "Schrems II", the European Court of Justice clarified that personal data of EU citizens may only be transferred to third countries outside the European Economic Area if they enjoy an essentially equivalent level of protection in that third country as in the EU. It found that the US does not have such an adequate level of protection. As shown, despite this clear court decision, the defendants transfer personal data of the plaintiff to the USA many times, including to the 2nd defendant. There is no justification in European or national law for any of these processing operations.

The fact that the defendants, contrary to their obligation under art. 13 para. 1 lit. f of the GDPR, provide neither information on the details of the data transfer using the 1st defendant's technical standards to the 2nd defendant in the USA, nor information on the required protective measures or appropriate or adequate safeguards, fits seamlessly into the picture of the intentional breach of law that is evident in all of the defendants' acts.

If the court does not consider the plaintiff's submissions or offers of evidence to date to be sufficient, or if it does not share the legal opinion represented here, it is expressly requested that the plaintiff be informed accordingly - if necessary by telephone - in accordance with section 139 ZPO.

Peter Hense	Tilman Herbrich	Elisabeth Niekrenz
(Lawyer)	(Lawyer)	(Lawyer)

Attachments

Annex K 1	Processing of plaintiff's Personal Data Triggered by Visit to 3rd defendant's website, Privacy Scandal: Secret Google Websites to Sell User Data?, URL: https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten, pp. 28-79 of the application,
Annex K 2	Entire printout of defendant 3's website privacy information as of 3/22/2021, available at https://onlinemarketing.de/datenschutzerklaerungen, accessed 3/22/2021,
Annex K 3	Processing of particularly sensitive data triggered by visiting the website of defendant 3's, Does my job endanger my health?, URL: https://onlinemarketing.de/karriere/unternehmenskultur/gefahrdet-mein-job-meine-gesundheit-corona-ruckenschmerzen-stress-risikofaktoren-arbeitsplatz, p. 95-104 of the application,
Annex K 4	Partial printout of defendant 1's website as of 03/23/2021 via IAB Tech Lab Members, available at: https://iabtechlab.com/about-the-iab-tech-lab/iab-tech-lab-members/, last accessed 03/23/2021,
Annex K 5	Partial printout of the website of the defendant 1: press release of 09.06.2020, available at: https://iabtechlab.com/press-releases/tech-lab-increases-investment-presence-in-europe/, last accessed on 12.02.2021,
Annex K 6	Partial printout of the website of vonwersch Digital Strategies GmbH as of 12.02.2021 on Tech Lab Leadership, available at: https://vonwerschpartner.com/case-studies/iab-tech-lab, last accessed on 12.02.2021,
Annex K 7	Partial printout of the website of the defendant 1, European Communication Groups, as amended on 23.03.2021, available at: https://iabtechlab.com/eea/, last accessed on 23.03.2021,
Annex K 8	Partial printout of Xandr, Inc. website, Platform Privacy Policy, as amended 2/24/2021, available at: https://www.xandr.com/privacy/platform-privacy-policy/ last accessed 4/14/2021,
Annex K 9	Printout of the extract from the commercial register of defendant 2 dated 23.03.2021,
Annex K 10	Partial printout from defendant 3's website, Gau: Secret Google Websites to Sell User Data?, Sept. 05, 2019, available at: https://onlinemarketing.de/technologie/datenschutzskandal-geheime-google-websites-verkauf-nutzerdaten, last accessed on April 14, 2021,

Annex K 11	Entire Printout of defendant 1's Website , Standard Header Container Integration with an Ad Server, as amended June 2017, available at: https://iabtechlab.com/wp-content/uploads/2016/07/IABTechLabStandardHeaderContainerIntegrationwithanAdServer_DRAFTforpubliccomment.pdf, last accessed 03/23/2021,
Annex K 12	Entire printout of defendant 1's website , Pubvendors.json v1.0: Transparency & Consent Framework, as amended May 2018, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md, last accessed 03/23/2021,
Annex K 13	Partial printout of Xandr, Inc. website: Third Party Providers, as amended 12/01/2021, available at https://docs.xandr.com/bundle/service-policies/page/third-party-providers.html#ThirdPartyProviders-Ad-serverPartners, last accessed 3/24/2021,
Annex K 14	Partial Printout of 1st defendant's Technical Specifications, OpenRTB Specifications v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#object_request, last accessed Feb. 11, 2021,
Annex K 15	Partial Printout: Example of Bid Request under 1st Defendant's Technical Specifications, OpenRTB Specification v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#bidrequest, last accessed Feb. 11, 2021,
Annex K 16	Entire printout of 1st defendant's Technical Specifications, OpenRTB Specification v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#, last accessed 03/26/2021,
Annex K 17	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_geo, last accessed 03/24/2021,
Annex K 18	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_site, last accessed 03/24/2021,

Annex K 19	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_publisher, last accessed 03/22/2021,
Annex K 20	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_user, last accessed 03/24/2021,
Annex K 21	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_data, last accessed 03/22/2021,
Annex K 22	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_segment, last accessed 03/22/2021,
Annex K 23	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_device, last accessed 03/24/2021,
Annex K 24	Entire printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md, last accessed 03/24/2021,
Annex K 25	Entire printout of 1st defendant's website, Implementation Guide for Brand Suitability with the Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/wp-content/uploads/2020/12/Implementation_Guide_for_Brand_Suitability_with_IABTechLab_Content_Taxonomy_2-2.pdf), accessed 03/23/2021,
Annex K 26	Printout of the home page of the 3rd defendant's website at the URL www.onlinemarketing.de displaying the console for web developers of the standard browser Chrome on 25.03.2021,
Annex K 27	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25/03/2021 showing the network connections (server request) with defendant 2,

Annex K 28	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25/03/2021 showing the network connections (server request) with defendant 2 and the web memory of the browser,
Annex K 29	Partial printout of defendant 2's website, "User ID Syncing with External Partners," as amended 03/31/2021, available at: https://docs.xandr.com/bundle/invest_invest-standard/page/topics/user-id-syncing-with-external-partners.html, accessed 03/31/2021,
Annex K 30	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25/03/2021 showing the network connections (server request) with defendant 2,
Annex K 31	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25/03/2021 showing the network connections (server request) with defendant 2,
Annex K 32	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25/03/2021 showing the network connections (server request) with defendant 2,
Annex K 33	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25.03.2021 under display of a server request for the submission of a bid request by defendant 2
Annex K 34	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the details for the 2nd defendant's server request.)
Annex K 35	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the details for the bid requests by the 2nd defendant.)
Annex K 36	Entire Printout of defendant's Integration Guide for SSPs, Incoming Bid Requests from SSPs, as amended Feb. 5, 2021, available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed Mar. 29, 2021,
Annex K 37	Entire printout of 1st defendant's Technical Specifications, OpenRTB API Specifications Version 2.4, as amended March 2016, available at: https://iabtechlab.com/wp-content/uploads/2016/04/OpenRTB-API-Specification-Version-2-4-FINAL.pdf, last accessed 03/29/2021,
Annex K 38	Partial Printout of defendant's Integration Guide for SSPs, Incoming Bid Requests from SSPs, as amended Feb. 5, 2021, available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed Mar. 25, 2021,

Annex K 39	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the 2nd defendant's server response with details of the Real Time Bidding auction conducted.
Annex K 40	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25.03.2021 showing the duration between server request and server response of the 2nd defendant with details of the Real Time Bidding auction conducted
Annex K 41	Partial printout of the website archive file (HAR file) of the website of defendant 3 dated 25.03.2021 showing the server response of defendant 2 with modified details of the Real Time Bidding auction conducted
Annex K 42	Partial printout of the website archive file (HAR file) of the website of defendant 3 from 25.03.2021 under display of the network connections (server request) with OpenX
Annex K 43	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 displaying the server request to conduct a Real Time Bidding auction using OpenX,
Annex K 44	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 displaying the server request to conduct a Real Time Bidding auction using OpenX,
Annex K 45	Partial printout of integration guide from online advertising exchange OpenX for DSPs, OpenRTB API, as amended Jan. 16, 2019, available at: https://docs.openx.com/demand-partners/ox-openrtb/#how-real-time-bidding-works, last accessed Mar. 29, 2021,
Annex K 46	Entire printout of 1st defendant's Protocol Technical Specifications, OpenRTB API Specifications Version 2.5, December 2016, available at: https://iabtechlab.com/wp-content/uploads/2016/07/OpenRTB-API-Specification-Version-2-5-FINAL.pdf, last accessed 03/23/2021,
Annex K 47	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing OpenX's server response with amended details of the Real Time Bidding auction conducted,
Annex K 48	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the time duration between server request and server response from OpenX with details of the Real Time Bidding auction conducted,
Annex K 49	Partial printout of website archive file (HAR file) of defendant 3's website dated 25/03/2021 showing network connections (server request) with BidSwitch,

Annex K 50	Partial printout of the website archive file (HAR file) of the defendant 3's website dated 25.03.2021 showing the network connections (server request) with SmartAdServer ,
Annex K 51	Partial printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/supplier-protocol.html , last accessed 26/03/2021,
Annex K 52	Entire printout of the integration guide from online advertising exchange BidSwitch for DSPs BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/supplier-protocol.html , last accessed on 26/03/2021,
Annex K 53	Partial website printout at URL https://www.bidswitch.com, last accessed 03/26/2021,
Annex K 54	Partial printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/rtb-ssp/context-pub.html, last accessed 26/03/2021,
Annex K 55	Partial printout of integration guide from online advertising exchange BidSwitch for DSPs, BidSwitch Supplier Protocol v3.0, available at: https://protocol.bidswitch.com/rtb-ssp/context-data.html, last accessed 26/03/2021,
Annex K 56	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the server response from SmartAdServer via BidSwitch with details of the Real Time Bidding auction conducted,
Annex K 57	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 25/03/2021 showing the duration between server request and server response from SmartAdServer with details of the Real Time Bidding auction conducted via BidSwitch,
Annex K 58	Information Commissioner's Office, Update report into adtech and real time bidding, available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, last accessed 10/02/2021,
Annex K 59	Partial printout of letter from Townsend Feehan, CEO of IAB Europe A.I.S.B.L., 26.06.2017, available at: https://www.iccl.ie/wp-content/uploads/2020/10/IAB-to-Commission-email-and-attachment-26-June-2017.pdf (archived), retrieved 24.03.2021,

Annex K 60	Letter from Townsend Feehan, CEO of IAB Europe A.I.S.B.L., June 26, 2017, available at: https://www.iccl.ie/wp-content/uploads/2020/10/IAB-to-Commission-email-and-attachment-26-June-2017.pdf (archived), accessed 04/15/2021,
Annex K 61	Entire printout from indexexchange.com website, Meropol, Meeting 2020's Business Challenges with Machine Learning, IX Traffic Filter, Aug. 06, 2020, available at: www.indexexchange.com/ix-traffic-filter-meeting-2020s-business-challenges-with-machine, last accessed Mar. 24, 2021,
Annex K 62	Entire printout from PubMatic website, Jain, Optimizing data processing at scale, 10/06/2020, available at https://pubmatic.com/blog/optimizing-data-processing-at-scale, retrieved on: 24.03.2021,
Annex K 63	Google website printout: OpenX: Power the future of advertising with Google Cloud, available at: https://cloud.google.com/customers/openx, last accessed 24/03/2021,
Annex K 64	Entire printout from Google's website, OpenRTB Integration, available at: https://developers.google.com/authorized-buyers/rtb/openrtb-guide, last accessed 03/24/2021,
Annex K 65	Full text from IAB Europe A.I.S.B.L. website, IAB Europe Transparency & Consent Framework Policies, version 2020-08-24.3.2, 2019, available at: https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf, accessed 24/03/2021,
Annex K 66	Partial printout from IAB Europe A.I.S.B.L. website, IAB Europe Transparency & Consent Framework Policies, version 2020-08-24.3.2, 2019, available at: https://iabeurope.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf, p. 11, retrieved 23/03/2021, p. 21,
Annex K 67	Full text of defendant 1's Public Comment, Tech Lab introduces additional consumer privacy safeguards into content and audience taxonomies, Apr. 30, 2020, available at: https://iabtechlab.com/blog/tech-lab-introduces-additional-consumer-privacy-safeguards-into-content-and-audience-taxonomies/, last accessed Mar. 24, 2021,
Annex K 68	Partial Printout of the Technical Specifications of 1st defendant's Protocol , IABTechLab, Inc, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object_eids, last accessed 03/24/2021,

Annex K 69	Partial Printout of 1st defendant's Protocol Technical Specifications, OpenRTB Specification v3.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB%20v3.0%20FINAL.md#objectmodel, accessed 03/24/2021,
Annex K 70	1st defendant's website's entirety: "Terms of Use," as amended Dec. 10, 2014, available at: https://iabtechlab.com/terms-of-use/, last accessed Mar. 24, 2021,
Annex K 71	Partial printout of defendant's website dated 03/24/2021, available at: https://ortbvalidator.iabtechlab.com/login last accessed 03/24/2021.
Annex K 72	Entire printout of defendant 1's website, Data Transparency Standard 1.0, as amended on 06/27/2019, available at: https://iabtechlab.com/wp-content/uploads/2019/06/Data-Transparency-Standard-1.0-Final-June-2019.pdf, last accessed on: 03/24/2021, partial printout of Defendant's website as of 03/24/2021, available at: https://ortbvalidator.iabtechlab.com/login last accessed on 03/24/2021,
Annex K 73	Partial printout of the website Adzine.de, Xander - Infrastructure for the global advertising ecosystem, available at: https://www.adzine.de/techfinder/xandr/, retrieved on 24.03.2021,
Annex K 74	Partial printout of 2nd defendant's website, OpenRTB Specs, as amended 03/22/2021, available at: https://wiki.xandr.com/display/supply/OpenRTB+Specs, last accessed 02/22/2021,
Annex K 75	Partial printout of 2nd defendant's website, Documentation Center: OpenRTB Integration Process, as amended 03/29/2021, available at: https://wiki.xandr.com/display/supply/Integration+Process, last accessed 03/29/2021,
Annex K 76	Partial printout of the website of the defendant 2, Documentation Center: Publisher Services, as amended 01.04.2021 available at: https://docs.xandr.com/bundle/xandr-api/page/publisher-service.html, last accessed 29.03.2021,
Annex K 77	Partial printout of 2nd defendant's website, Documentation Center: How Integration Works, as amended 03/25/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/how-integration-works.html, last accessed 03/25/2021,
Annex K 78	Partial printout of 2nd defendant's website, Documentation Center: User ID Mapping, as amended 03/25/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/user-id-mapping.html, last accessed 03/25/2021,

Annex K 79	Printout of the website of defendant 3 at the URL: https://onlinemarketing.de/karriere/unternehmenskultur/gefahrdet-mein-job-meine-gesundheit-corona-ruckenschmerzen-stress-risikofaktoren-arbeitsplatz under display of the console for web developers of the standard browser Chrome from 01.04.2021,
Annex K 80	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 01.04.2021 showing the network connections (server request) with Adform,
Annex K 81	Partial printout of the website archive file (HAR file) of the website of defendant 3 from 01.04.2021 under display of the network connections (server request) with Adform and the web memory of the browser of the plaintiff,
Annex K 82	Partial printout of website archive file (HAR file) of defendant 3's website dated 25/03/2021 showing network connections (server request) using Adform,
Annex K 83	Partial printout of Adform's integration guide for incorporating tracking code to create categories for website owners, as amended 03/19/2019, available at: https://www.adformhelp.com/s/article/UUID-7539fb22-b0ff-e321-b3f3-72e007106d9a, last accessed 04/06/2021,
Annex K 84	Partial printout of presentation slides by Adform's former Senior Product Director Adform Audience Products, Ashu Mathura, available at: https://i.iinfo.cz/files/iac/449/ashu-mathura-adform-1.pdf, last accessed 04/06/2021,
Annex K 85	Partial printout of the website archive file (HAR file) of defendant 3's website dated 01.04.2021 showing the network connections (server request) with Yieldlove,
Annex K 86	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 01.04.2021 showing the server response with details of the Real Time Bidding auction conducted,
Annex K 87	Partial printout of the website archive file (HAR file) of the 3rd defendant's website dated 01.04.2021 showing the time duration between server request and server response with details of the Real Time Bidding auction conducted,
Annex K 88	Entire printout of 1st defendants' website, Final Audience Taxonomy v1.1 and Content Taxonomy v2.1 provide additional consumer privacy safeguards, as amended 09/07/2020, available at: https://iabtechlab.com/blog/final-audience-content-taxonomies-provide-additional-consumer-privacy-safeguards/, accessed 03/24/2021,
Annex K 89	Printout of email from Benjamin Dick to plaintiff dated 8/27/2020.

Annex K 90	Partial Printout of 1st defendant's Technical Specifications, Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/standards/content-taxonomy/, last accessed 03/22/2021,
Annex K 91	Partial Printout of 1st defendant's Technical Specifications, Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/standards/content-taxonomy/, last accessed 03/22/2021,
Annex K 92	Full printout of 1st defendant's technical specification, Content Taxonomy v2.2, as amended December 2020, available at: https://iabtechlab.com/standards/content-taxonomy/, last accessed 03/22/2021,
Annex K 93	Partial printout of 2nd defendant's website, Incoming Bid Request from SSPs, as amended 06/04/2021, available at: https://docs.xandr.com/bundle/supply-partners/page/incoming-bid-request-from-ssps.html, last accessed 06/04/2021.
Annex K 94	Entire printout of 1st defendant's website, Audience Taxonomy, as amended April 2020 available at: https://iabtechlab.com/standards/audience-taxonomy/, accessed 03/24/2021,
Annex K 95	Partial Printout of 1st defendant's Technical Specifications, Audience Taxonomy v1.0, as amended May 2018, available at: https https://iabtechlab.com/standards/audience-taxonomy/ last accessed 03/23/2021,
Annex K 96	Partial Printout of 1st defendant's Technical Specifications, Audience Taxonomy v1.0, as amended May 2018, available at: https https://iabtechlab.com/standards/audience-taxonomy/ last accessed 03/23/2021,
Annex K 97	Partial Printout of 1st defendant's Technical Specifications, Audience Taxonomy v1.0, as amended May 2018, available at: https://iabtechlab.com/standards/audience-taxonomy/ last accessed 03/23/2021,
Annex K 98	Entire Printout of 1st defendant's Technical Specifications, Audience Taxonomy v1.0, as amended May 2018, available at: https://iabtechlab.com/standards/audience-taxonomy/ last accessed 03/29/2021,
Annex K 99	Partial Printout of 1st defendant's Technical Specifications, Audience Taxonomy v1.1, as amended April 2020, available at: https://iabtechlab.com/standards/audience-taxonomy/, last accessed 03/24/2021,

Annex K 100	Entire Printout of 1st defendant's Technical Specification, Audience Taxonomy 1.1, as amended April 2020, available at https://iabtechlab.com/standards/audience-taxonomy/, last accessed Feb. 12, 2021,
Annex K 101	Partial Printout of 1st defendant's Technical Specification, Transparency and Consent String with Global Vendor & CMP List Format, as amended December 2019, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#the-core-string, accessed 03/24/2021,
Annex K 102	Entire Printout of 1st defendant's Technical Specification, Transparency and Consent String with Global Vendor & CMP List Format, as amended December 2019, available at: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#the-core-string, accessed 03/24/2021,
Annex K 103	Partial Printout of 1st defendant's Technical Specifications, AdCOM Specifications v1.0, as amended June 2020, available at: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object--extended-identifiers-, last accessed 03/24/2021,
Annex K 104	Entire printout of 3rd defendant's website, Privacy Information, as amended 03/25/2021, available at: https://onlinemarketing.de, last accessed 03/25/2021,
Annex K 105	Partial Printout of 3rd defendant's website, Privacy Settings, as amended 3/24/2021, available at https://onlinemarketing.de, last accessed 3/24/2021,
Annex K 106	Entire Printout of 3rd defendant's website, Privacy Settings, as of 03/25/2021, available at https://onlinemarketing.de, last accessed 03/25/2021,