UiO : Faculty of Law
University of Oslo

Joint controllership for third-party tracking cookies

An assessment of whether and what types of third-party tracking cookies could invoke joint controllership under GDPR, and how this would affect the division of information obligations and liabilities under ePD and GDPR.

Candidate number: 7018

Submission deadline: 01.12.2019

Number of words: 16451

Table of contents

ABSTRACT

This thesis considers the plausibility and effect of joint controllership under the European Data Protection Framework for website operators when placing third-party tracking cookies. Traditionally, these cookies have only given rise to a controller-processor relationship between the website operator and third-parties. The recent rulings of the CJEU has broadened the definition of joint controllership, making it questionable whether website operators are always confined to the roles of processors or controllers when placing third-party tracking cookies. If joint controllership is likely, this will affect what information obligations and liabilities rests with the parties and what can be lawfully divided between them. By analyzing the defining criteria for controllership and assessing the obligations and liabilities arising from the legal framework, the author seeks to illuminate when third-party tracking cookies invoke joint control and what practical impact this has.

GDPR; ePrivacy Directive; joint control; information rights; liability

ABBREVIATIONS

CJEU	European Court of Justice
DPA	Data Protection Authority
DPAg	Data Processing Agreement
DPD	Directive 95/46/EC (Data Protection Directive)
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisory
ePD	Directive 2002/58/EC (ePrivacy Directive)
ePR	(forthcoming) ePrivacy Regulation
GDPR	Regulation 2016/2017
OTTs	Over-the-top services
SA	Supervisory Authority
SCC	Standard Contractual Clauses
The New Framework Directive	Directive 2018/1972
The Old Framework Directive	Directive 2002/21/EC
WP29	Article 29 Working Party

1 Introduction

Since the Internet became publicly available in 1991 it has become the main source for information dissemination, communication, entertainment and to a large extent commerce and business on a world-wide scale.[1] Given the rapid digitization of society and the constant emergence of new online technologies, lawmakers around the world have been kept busy attempting to regulate the online environment in a manner corresponding to the rights and obligations imposed in the physical world.

In the online rat-race for consumers' attention, the concept and power of *big data* has become a particularly pressing matter for legislators. Over the past decades up until today, individuals have generated – and are generating - vast amounts of data online. This is because they potentially leave digital traces that either telecom companies or online actors can utilize.[2] Examples include browsing habits, search history, location data and site interactions revealing for instance personal preferences, age, occupation and gender. Big data is deemed any data that are large in volume, consist of a variety of types of data from potentially different sources, are produced at high rates, have quantifiable value to anyone utilizing it and where the veracity – or correctness- of the data can be assessed.[3]

The reason for this peaked interest is the concern for the right to privacy of online users, or even the right to data privacy now witnessed under the Charter of the European Union. Granted the capacities of online actors to collect digital traces of individuals, all or parts of the information may constitute personal data capable of identifying the user.

Within the European Union, the processing of personal data has been regulated since the initial Directive 95/46/EC. Since then, the data protection framework has expanded and is currently being renewed, as an effort to account for the ever-changing technological developments in the online world.

Within this refreshed framework, the use and placement of cookies and similar technologies has been granted significant attention. Cookies, or *magic cookies*,[4] is computer jargon for a small text file, or a so-called identifier, that is stored on a user's device upon using an online

[1] Barry M. Leiner, 'A Brief History of the Internet' (2009) vol 39 issue 5 ACM SIGCOMM Computer Communication Review p 22

[2] Keith Gordon, 'What is Big Data?' (2013) vol 55 issue 3 ITNow p 12

[3] *ibid*

[4] Eric S. Raymond, *The New Hacker's Dictionary* (3rd edn, MIT Press 1996), term 'magic cookie'

service.[5] These store information during and in between website visits for various reasons. Some are used to optimize the experience of the website, for instance by remembering log-in information or what a user adds to their shopping basket on that particular site. Others are used to track browsing behavior to create profiles on the user and/or to provide targeted advertising. The latter cookies are defined as tracking cookies, a form of *persistent* cookies which are active in between visits to websites and remain stored after closing the browser.[6] While the former category of cookies is given appropriate consideration under the framework, the latter category is heavily considered and, unfortunately, prone to problems.

Tracking cookies have proven to be a prickly point in data protection law, especially *third-party* tracking cookies. First-party and third-party cookies are distinguished by which domain owns the cookie placed on the website. In the case of first-party cookies, it is the website operator himself that stores or accesses the cookie on the user's terminal equipment. In the case of third-party cookies, the website operator sets cookies belonging to *other* domains. An example is Google's Analytics or Adsense cookies, tracking cookies often set by website operators other than Google itself.

Today, cookies are mainly governed by Directive 2002/58/EC ("**ePD**"), infamously known as the "cookie law" and Regulation 2016/679 ("**GDPR**"), replacing Directive 94/46/EC ("**DPD**"). Both instruments impose certain obligations and responsibilities on the website operator and the cookie provider towards visitors. When third-party tracking cookies process personal data, the obligations and responsibilities resting on each party depends on whether the they possess the role as a *processor*, *controller* or *joint controller* under the GDPR, including what the mandatory contractual arrangement under the instrument permits or restricts them from delegating between them. Determining what role each party possesses is therefore imperative to ensure compliance.

A controller is someone who determines the purposes and means for processing; a processor is merely processing the data on behalf of the controller and without any influence on the purposes and means; and a joint controller plays a part – either minor or major – in determining or influencing the purposes and means.[7] Historically, website operators and third parties have generally been classified as either controller or processor when setting and utilizing third-

---

5 David M. Kristol, 'HTTP Cookies: Standards, Privacy and Politics' (2001) vol 1 issue 2 ACM Transactions on Internet Technology p 151-198

6 Netscape.com, 'Persistent Client State HTTP Cookies' (curl.haxx.se) <https://curl.haxx.se/rfc/cookie_spec.html> accessed 22 November 2019

7 Council Regulation (EC), Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") OJ L 119 arts 4(7)-(8) and 26

party cookies. In comparison to DPD, the GDPR introduced changes to these concepts, and the concept of joint control has especially been prone to expansion through recent case law. As a consequence, there is a debate in the online community as to whether and when a web-site operator can be a joint controller with third parties when it sets their tracking cookies. If joint controllership is possible or even plausible in this context, this will undoubtedly affect the obligations and responsibilities of the parties.

This thesis aims to assess whether and when website operators can be joint controllers with third parties when placing third-party tracking cookies, and to inspect how this will affect the contractual arrangement or agreement between the parties in relation to the division of information obligations and liabilities under ePD and GDPR.

1.1 Agenda

Chapter 2 will set out the legal landscape in which cookies are placed. This entails a review of the material and territorial scope of the instruments, in addition to what the interplay between ePD and GDPR means in the context of third-party tracking cookies. This is imperative in order to understand the extent to which both instruments apply and will be particularly important when we inspect the shift in information obligations and liabilities from controller-processor relations to joint controllership in chapter 4.

Chapter 3 will elaborate on the concepts of controllers and processors under GDPR, and the significance of the broadening scope of joint controllership. The chapter will assess whether placing third-party tracking cookies can invoke joint controllership, and if so what types of tracking cookies this concerns.

Chapter 4 will explore the information obligations and liabilities under ePD and GDPR, including how the division of these will differ in joint controller relationships as compared to controller-processor relationships. Here, the duties provided under the instruments will be set out and reviewed in relation to who they belong to by text, and how they can be divided in the different contractual arrangements. The relevance of exploring these two duties are to see how joint controllership would affect the placement and use of third-party tracking cookies *in practice*.

Chapter 5 will summarize the findings of this paper, reflecting on the plausibility and effect of joint controllership.

1.2 Scope of paper

1.2.1 Limitation of scope

Joint controllership would give rise to a myriad of questions in the context of tracking cookies. Which cookies that are caught and how liabilities and information obligations could be divided are only three pieces of the puzzle, yet arguably constitute some of the crown pieces.

The thesis will not explore issues related to enforcement or technical or organizational requirements to protect personal data under the instruments, nor any obligations concerning the security of the processing. It will, to some extent, touch upon the extraterritorial scope of the GDPR but will not elaborate on the issues of extraterritorial enforcement. Sanctions for non-compliance will briefly be discussed but will be limited to the division of responsibilities and liabilities between controllers, processors and joint controllers.

Lastly, it is worth noting that other information obligations outside the ePD and GDPR may apply to the parties, such as in the EU-US Privacy Shield, in privacy seal programs (e.g. TRUSTe and EuroPriSe) and in industry association standards (e.g. Network Advertising Initiative, Digital Advertising Alliance). These will not be discussed in this paper. This equally applies to instances where liability arise outside the data protection context, such as in the case of tort law, criminal law or contract law. Contractual liability will mainly be discussed insofar as this is related to provisions under the GDPR.

1.3 Cookies explained

1.3.1 Cookies to be understood as 'cookies and similar technologies'

EU data protection law employs a technology-neutral language in order to capture a broad range of tech-solutions capable of processing personal data. Thus, neither ePD or GDPR contain provisions expressly directed at cookies. GDPR frequently refers to ‘online identifiers’, while ePD is more hinged on *any* type of technology capable of storing or accessing information on the user’s device.

These descriptions can be somewhat merged. Any tech that stores or accesses information (that is deemed personal data) on the user’s device is an online identifier. A cookie is only one type of such technology, but it is the most popular solution offered. Much of the similar technology functions in the same way as cookies but is built on other codes and may collect different types of user information.

Examples of such technology include Flash cookies, tracking pixels, local storage, web beacons and scripts. To signify the importance of a technology-neutral language in EU data protection law, we can refer to the concerns of the Article 29 Working Party ("**WP29**") on the use

of Flash cookies, as these cannot be deleted through traditional privacy settings and could potentially restore traditional HTTP cookies that were erased or rejected by users.[8]

The inclusion of similar technologies under the term 'cookies' is therefore necessary for the purpose of this discussion, as the findings herein will equally apply to these forms of tracking technologies.

1.3.2 Third-party tracking cookies and their purposes

Tracking cookies (and similar technologies) are defined as *persistent* cookies that can be read across two or more website domains, whereof the reason is to collect information for a specified purpose. This occurs when several websites have partnered up with a third-party and have their cookie embedded into the website code. Thus, depending on the type of tracking cookie, visiting sites that have the cookie available will cause information from the user's visits to be stored in the one and same cookie. Often, major third-parties have the capacity to gain information from a combination of different cookies (and similar technologies) which can later be compiled to create a larger profile or identify unique users.[9]

Third parties providing tracking cookies often do so for various purposes, and it usually is for the benefit of both parties. In the case of collecting information for statistical or analytical purposes, websites can place tracking cookies to collect information on for instance website visits or interaction with their ads on different websites. These services are often provided either at a freemium rate, or for larger companies demanding more in-depth tools, a considerable monetary amount. Examples include the standard Google Analytics and Analytics 360.

In other instances, such as in the case of behavioral targeting and advertising regimes, the website operator displays ads on behalf of a third-party, whereof the content of the ad is based on its relevance to the user. Here, the third-party targets the visitor on the basis of the information collected by a tracking cookie(s), meaning it creates a profile of the user including for instance his interests, age group, sex or level of income.[10] The website displaying ads on behalf of the third-party is then paid either for the actual advertising space, per impression, per

---

[8] Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' (WP 171, 22 June 2010) p 6

[9] Steven Englehardt, Arvind Narayanan, 'Online Tracking: A 1-million-site Measurement and Analysis' (2016) Princeton University p 2 <https://chromium.woolyss.com/f/OpenWPM-1-million-site-tracking-measurement.pdf> accessed 22 November 2019

[10] Niklas Schmücker, 'Web Tracking – SNET Seminar Paper Summer Term 2011' (2011) Berlin University of Technology p 2 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.8976&rep=rep1&type=pdf> accessed 22 November 2019

click or per sale.[11] This arrangement requires a trade-off: websites must embed tracking cookies in order for the third-party to provide relevant ads.

This latter instance often involves the use of adtech and real time bidding ("RTB"). Adtech is defined as "*tools that analyse and manage information for online advertising campaigns and automate the processing of advertising transactions*".[12] RTB, on the other hand, uses these tools to permit the purchase and sale of ads in real time, meaning that the ad selection for a particular page and a particular visitor happens instantly upon visiting the website. The information collected from the cookie is baked into a bid request, where advertisers will bid in an open auction on an impression basis (i.e. one presentation of the ad). If the information baked into the unique bid request reveals that the individual is a young woman engaging with a lot beauty content and products, beauty advertisers will likely compete for this bid. In these processes, revenues benefit both the third party providing the service, the advertisers and the publishers.[13] Examples includes Googles AdSense and AdRoll, who own the cookies underpinning the RTB process.

Finally, there are instances where a website may host "widgets", for instance Facebook or Instagram "like" buttons, which may permit the third-party (i.e. Facebook or Instagram) to track the user through cookies across the websites who have this button.[14] In return, the website may increase their exposure on such platforms.

2 Legal Background

2.1 The EU Data Protection Framework Reform and cookies

Cookies of all types are mainly regulated under Directive 2002/58/EC, amended by Directive 2009/136/EC ("**ePD**"), infamously known as the "cookie law". The ePD interplays with Directive 2002/21/EC ("**the old Framework Directive**"), and Directive 95/46/EC ("**DPD**"), now replaced by Regulation 2016/679 ("**GDPR**"). Any definitions not already set out in the ePD is to be read in light of definitions provided under the Framework Directive and the

[11] *ibid*

[12] Information Commissioner's Office, 'Update report into adtech and real time bidding' (2019) p 8 <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed 18 November 2019

[13] See e.g. Google, 'About bidding on AdSense' <https://support.google.com/adsense/answer/190436?hl=en&ref_topic=1628432> accessed 15 November 2019

[14] Richard Gomer and others, 'Network Analysis of Third Party Tracking, User Exposure to Tracking Cookies through Search' (2013), vol 1 Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT) p 550

GDPR.[15] In the case of tracking cookies processing personal data, the general provisions of the GDPR will apply in *addition* to the cookie requirements under ePD. It is under the former instrument that the concepts of controllers, processors and joint controllers become relevant. The reason why both instruments must be discussed is that they are intertwined and can affect the division of responsibility and tasks between the roles. That is particularly true as the entry into force of GDPR has affected how the ePD requirements are to be interpreted.

The old Framework Directive has recently been repealed and replaced with Directive 2018/1972 ("**the new Framework Directive**"). This is to be transposed into national law before 21 December 2020. Article 125 provides that references to the repealed Directive shall be construed as references to the new Framework Directive.[16] While the new Framework Directive certainly will expand the scope of application of the ePD to other equivalent online services, such as "over-the-top" services ("**OTTs**"), this expansion will not impact its existing applicability to website operators (see subchapter 2.2.1). As website operators are the prime target of this analysis, an elaboration of this subject will not be appropriate for this thesis.

Of the instruments relevant to cookies, the ePD is the only one that has not yet been renewed. It was supposed to be replaced by an ePrivacy Regulation ("**ePR**") at the same time as the GDPR came into force and was deemed a necessity to "*reinforce trust and security in the Digital Single Market*".[17] However, this ambition was never met due to the lack of agreement on key provisions. Seeing that the resolution of these issues is still ongoing, it appears it may take yet a few years before we will see an ePrivacy Regulation enter into force.

The halt in the framework reform may be a partly causative factor as to why the obligations on website operators are difficult to foresee. The ePR might relieve the patchwork of national implementation of the ePD by harmonizing the interpretation of the requirements to setting and utilizing cookies. On the other hand, it may not, as its interplay with the GDPR will still exist. It is mainly the latter instrument that has caused the controversy on what the requirements to cookies under ePD are or which general obligations rests with – or may be delegated to – what parties in the case of third-party tracking cookies. All these points will likely remain unaffected under the ePR. A remedial point might be that the GDPR is vowed to be reviewed

---

[15] Council Directive (EC), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector art 2

[16] Council Directive (EC), Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code art 125

[17] Council of the European Union, '9292/1/19 Rev 1: Note from the Presidency to the Delegations' (Brussels, 20 May 2019) p 2 <https://www.politico.eu/wp-content/uploads/2019/05/Progress-report-v2-May.pdf> accessed 9 November 2019

once the ePR comes into existence,[18] not to mention the continuous efforts to clarify its provisions through guidelines and case law.

As the joint controller discussion and duties of the parties when setting third-party tracking cookies only arise in the context of ePD and GDPR, an introduction to how and when they apply to such cookies, including their interplay, will be explored in the following subchapters.

2.1.1 How Directive 2002/58/EC and Regulation 2016/679/EC apply to tracking cookies: material scope

The GDPR concerns the protection of natural persons with regard to the processing of personal data. The material scope of the GDPR is determined by the notions 'processing' of 'personal data', when such processing is a part of, or intended to be part of, a filing system.[19] The filing system can be electronic or manual and need only a simple structure (e.g. alphabetical ordering) to be considered as such.[20]

'Processing' is widely defined in the instrument, and essentially concerns *any* act carried out on personal data.[21] This includes for example collecting, storing, recording, distributing or making available.[22] The notion of 'personal data' is equally broad. It entails any information that relates to an identified or identifiable (living) person.[23] If the information alone or in collection with other information can lead to the identification of the person, either directly as an individual or as belonging to a specific group (e.g. age, occupation, place of residence),[24] this information is also considered personal data. Relevant examples of personal data are identification numbers, online identifiers such as cookies and IP addresses,[25] or dynamic IP addresses.[26]

---

[18] GDPR recital 173

[19] GDPR art 2

[20] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Springer 2017) p 11

[21] GDPR art 2(1)

[22] GDPR art 4(2)

[23] GDPR art 4(1), cf recital 27

[24] Article 29 Working Party, 'Opinion 1/2007 on the concept of personal data' (WP 136, 20 June 2013) p 13

[25] GDPR recital 30; C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI:EU:C:2011:771

[26] Voigt and Bussche (n 20); C-582/14 *Patrick Breyer v Germany* [2016] ECLI:EU:2016:779

The GDPR already recognizes cookies as a type of 'online identifier'.[27] If tracking cookies process any information that may constitute personal data, the material scope is invoked. WP29 has confirmed that this often is the case for tracking cookies.[28]

The ePD covers the same matters as GDPR, but particularize and complement the GDPR in the electronic communications sector. The material scope of ePD is only determined by the processing of personal data in connection with providing "*publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices*".[29] The notions 'processing' and 'personal data' are awarded the same meanings as in the GDPR.[30] 'Electronic communications services' are defined as services "*normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications network*".[31] It is important to highlight that 'normally provided' means that a payment is not necessary in order for the definition to apply. Thus, website operators providing a service over a publicly available electronic communications network (e.g. the Internet), whether it requires payment or not, is covered. This view is confirmed by EDPB,[32] and entails for instance news websites, social media sites and search engines providing free services.

The ePD has dedicated a stand-alone provision dealing with cookies. Art. 5(3) sets requirements to any technology storing or accessing information in the user's terminal equipment.[33] This is the very essence of what cookies and similar technologies do. What is unique about this provision is that it refers to any information, meaning that it applies even when the cookies collect non-personal data. Thus, irrespective of whether a tracking cookie does or does not collect personal data, the ePD will apply.

2.1.2 Situations in which both instruments apply: territorial scope

The GDPR applies to the processing of personal data in two instances. The first is when the processing is carried out "*in the context of the activities of an establishment of a controller or processor in the Union*".[34] The second is when the processing is carried out by controllers or

[27] GDPR recital 30

[28] WP29 Opinion 2/2010 (n 8) p 9

[29] ePD art 3

[30] ePD art 2; GDPR art 94(2)

[31] ePD art. 2(c)

[32] European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (12 March 2019) p 11

[33] ePD art 5(3)

[34] GDPR art 3(1)

processors established outside the EU, and it relates to either offering goods or services (regardless of whether payment is involved) or the monitoring of data subjects' behavior when the behavior finds place within the EU.[35] The former instance is relevant only to EU-based establishments, whereas the latter applies extraterritorially to non-EU based establishments.

For EU-based entities to fall within the territorial scope of the GDPR, they must be either a controller or processor, and form part of an 'establishment'. An 'establishment' refers to "*effective and real exercise of activities through stable arrangements*".[36] Its legal form or size of the activity is not decisive for determining the existence of an establishment.[37] Thus, if a third party or a website operator conducts a minor activity (e.g. sets third-party tracking cookie) through a stable arrangement, this suffices to fulfill the criteria. This may also be the case if either such party is based outside the EU but has an agent or single employee (deemed a controller or processor) based in the EU who acts "*with a sufficient degree of stability*".[38]

For non-EU based entities, however, they must either (a) provide goods or services (free or otherwise) targeting EU-based users or (b) monitor their behavior. It is often this latter category that invokes the applicability of the GDPR to tracking cookies. The reason is that tracking cookies collect certain information which is normally used for profiling and/or targeted/behavioral advertising.[39] Thus, if a non-EU entity seeks to set, access or utilize tracking cookies on an EU-based user's device, the parties are required to observe the obligations of the GDPR.

The ePD on the other hand, does not mention a territorial scope. This must therefore be deduced from its material scope. A variety of practices are covered by the material scope, which means that its territorial scope may vary depending on the actor and act in question.[40] This is not to say that the ePD can have an extraterritorial scope, as it does not explicitly refer to any such scenarios where that would be a plausible outcome. Given the resistance to the extraterritorial scope of GDPR, it would be even more difficult to argue in favor of such an interpretation.

---

[35] GDPR art 3(2)(a)-(b)

[36] GDPR recital 22

[37] C-230/14 *Weltimmo s.r.o v. Nemzeti Adatvédelmi és Információszabadság Hatóság* [2014] ECLI:EU:C:2015:639 para 31

[38] European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' (16 November 2018) p 5

[39] GDPR recital 24

[40] Tijmen H. A. Wisman, 'Privacy, Data Protection and E-Commerce' in Arno R. Lodder, Andrew D. Murray (ed), *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing Limited 2017) p 369

In the case of an EU based website operator offering a good or service (e.g. theguardian.co.uk providing news or nelly.com providing clothing) over the Internet, the territorial scope would be invoked. For a non-EU based website operator (e.g. Washington Post providing news, or hellomolly.com providing clothing), the ePD would not apply.

What can be deduced from the material and territorial scope of the instruments is that (a) if an EU based website operator places third-party tracking cookies (i) the ePD will always apply, and (ii) both the ePD and GDPR will apply if the cookie processes personal data; and (b) in the case of non-EU based website operator placing tracking cookies, (i) the ePD will never apply whereas (ii) the GDPR will apply if the tracking cookie processes personal data of EU based users and the tracking is deemed to monitor their behavior.

This thesis focuses on scenario (a)(i) and (ii), where both instruments apply.

2.1.3 Interplay between Directive 2002/58/EC and Regulation 2016/679/EC

When tracking cookies invoke both ePD and GDPR, it is important to understand their interplay prior to discussing the issue of joint controllership and the contractual division of obligations and liabilities.

Where article 2 of the ePD state that definitions not provided under the instrument is to be given same meaning as in the DPD,[41] the GDPR now requires that any references to the latter instrument is to be understood as references to the GDPR.[42] This has had a significant impact on interpreting the ePD requirements to setting tracking cookies, namely that of 'consent' and 'clear and comprehensive information'. Consent must now be a valid consent under the GDPR.

As stated, ePD only *'particularizes and complements'* the GDPR.[43] If tracking cookies invoke the material scope of the GDPR (i.e. they process personal data), the general provisions of that instrument will also apply. However, this dual application does not mean that the GDPR applies in its entirety. Article 95 GDPR comforts us that it only applies insofar as the specific subject matter is not already dealt with under the ePD.[44] The relationship between the two instruments is therefore a case of *lex-specialis-lex-generalis*.[45] For instance, as the ePD has set

[41] ePD art 2

[42] GDPR art 94(2)

[43] ePD art 1(2)

[44] GDPR art 95

[45] EDPB Opinion 5/2019 (n 32) p 13

out the specific rules concerning the lawful basis for setting cookies (i.e. consent), other lawful bases under the GDPR for the *same* subject-matter is to be disregarded.

However, ePD generally applies to the *access to or storing of* any information on the user's terminal equipment. Where tracking cookies collects information considered personal data, any subsequent processing is not covered by ePD. This happens when a third party wishes to process the data for another purpose than mere storage or access, such as creating profiles and/or improve relevancy of their targeted advertising. In such instances, both instruments require that the obligations and rights under the GDPR must be observed,[46] and their dual application has been confirmed by The WP29 and The European Data Protection Board ("**EDPB**").[47]

What this means for website operators and third parties is that additional obligations under the GDPR will often apply, for instance regarding the lawful basis, information to be provided, or measures pertaining to data subject's rights towards the data collected. In that sense, the general rules of the GDPR entail a larger palate of provisions to comply with than the ePD. Who is responsible for or liable under what provisions will depend on their role as either controller, processor or joint controllers under the GDPR, which is why the discussion is highly relevant to the placement of third-party tracking cookies.

2.2 CJEU case law relevant to cookies and joint controllership

To prepare the reader for the analysis of joint controllership in chapter 3 and information obligations in chapter 4, the key cases on cookie usage and cookie placement under GDPR and ePD will be presented.

The first case to touch upon joint controllership was C-210/16 *Wirtschaftsakademie*. Here, the court considered a Facebook fan page administrator to be a joint controller with Facebook for the personal data collected by cookies on its page. The cookies placed were for two purposes; (a) improvement of Facebook's advertising system and (b) the provision of statistics to the page administrator. Joint control was established because (a) the administrator gave Facebook the opportunity to place the cookies, (b) he contributed to the processing as he could toggle what data was to be collected for the statistics and (c) he benefitted from these associated services. The party's lack of access to the personal data processed was considered irrelevant for the assessment.[48]

[46] GDPR recital 173; ePD recital 10

[47] EDPB Opinion 5/2019 (n 32) p 11; WP29 Opinion 2/2010 (n 8) p 9

[48] C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C:2018:388

In the following case C-25/17 *Jehovah's Witnesses*, the court reconfirmed the irrelevance of access to the processed data for controllership to arise. The case concerned the collection of personal data by door-to-door preachers, whereof the community was held to be joint controller with its members for these activities. The court ruled that it exerted influence on the purposes and means of the processing activity as it was "organized, coordinated and encouraged" by that Community.[49]

The final and most recent case dealing with joint control is C-40/17 *Fashion ID*. The case concerned a website embedding a social plugin, which initiated the collection and transfer of personal data to a third-party. The court found the website to be a joint controller because he exerted decisive influence on the purposes of processing by permitting the collection and transmission of the data, and because both parties attained a mutual benefit from the activity.[50]

In all three cases, the court noted that joint control does not imply equal responsibilities for the processing activity at hand.

In relation to the provision of information under ePD, C-673/17 *Planet* 49 is the first case to illuminate the extent of these duties after GDPR replaced DPD. The judgment confirmed that (a) consent under ePD is to be interpreted as consent under GDPR, and that (b) the information to be provided to the user under article 5(3) ePD must include the duration of the cookies and, if third parties can access them, the identity of such parties.[51]

3 Controllers, processors... or joint controllers?

3.1 Why joint control may be problematic for third-party tracking cookies

Third-party tracking cookies have traditionally only invoked the roles of *controller-processor* or *processor-controller* between website operators and third parties. The rulings in *Wirtschaftsakademie* and *Fashion ID* have broken this tradition, by establishing joint controllership in certain types of cookie usage situations. In the former case this concerned the placement of cookies when making a Facebook fan page, whereas the latter concerned embedding a social plugin on a website entailing the collection and transfer of personal data. If joint controllership is invoked for third-party tracking cookies on a broader spectrum, this will affect the liabilities and obligations amongst the parties on essentially any online website. The

[49] C-25/17 *Jehovan todistajat* [2017] ECLI:EU:C:2018:551

[50] C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629

[51] C-673/17 *Planet 49* [2019] ECLI:EU:C:2019:801

reason is that third-party tracking cookies form a large part of the internet economy and is often an integral part of how most persons and entities conduct their online operations.

In controller-processor relationships and *vice-versa*, the GDPR requires the parties to enter into a contractual agreement or legally valid act under Union law, setting out the rights and obligations of the parties. This is referred to as a Data Processing Agreement ("**DPAg**"). Article 28 GDPR sets out the minimum requirements of such agreements, with some room to form the contract according to the parties wishes.[52] However, several restrictions apply in terms of what the processor can do.

In joint controller relationships, however, article 26 GDPR requires a different form of arrangement, where the parties have much more freedom to distribute the obligations between themselves.[53] Granted that both parties are controllers, this entails an increased responsibility both in terms of compliance and liability. Thus, a joint controller arrangement will require a more detailed effort for the parties to appropriately delegate compliance and risks – and even then, a few responsibilities will still apply irrespective of the arrangement.

As each relationship and role carries different obligations, the most important impact of a shift from controller-processor to joint controllership would be that there is an increased risk of non-compliance, which may invoke liability to pay compensation for damages and/or the imposition of administrative fines by the national supervisory authority ("**SA**"). Depending on the obligations breached, these fines can constitute up to 20 000 000 EUR or 4 % of the total world-wide annual turnover, whichever is higher.[54]

3.2 Defining controllers and processors

The distinction between who is a controller or processor comes down to who determines the purposes and means of a processing activity, being the controller, and who merely conducts the processing on behalf of another, being the processor.[55] By virtue of the broad definitions under the GDPR, nearly anyone can qualify as either a controller or processor. As long as the party is a natural or legal person, public authority or any other body, that element is fulfilled.[56] Thus, whether the website operator is a natural person or a corporation will not affect the clas-

[52] GDPR art 28
[53] GDPR art 26
[54] GDPR art 83(4)-(5)
[55] *ibid*
[56] GDPR art 4(7)-(8)

sification as either controller or processor. This can be exemplified by the *Lindqvist* case, where the CJEU found Ms. Lindqvist personally to hold controller responsibility.[57]

'Determining' denotes the party that decides on the processing activity. Following the *Jehovah's Witness* ruling, this also entails any party "exerting influence" over the processing of personal data for his own purposes.[58] Whether a party fulfills this criterion should not be determined solely by virtue of any legal obligations or formal appointment, but by the factual circumstances.[59] One such factual circumstance was elaborated in *Fashion ID*. Here, the court held that social plugins rendering the collection and processing of personal data possible constitute 'decisive influence'.[60] Apart from that example, the WP29 and the European Data Protection Supervisor ("**EDPS**") have located three questions that should be asked when assessing the factual influence of a party:

1) why is the processing takes place?
2) who initiated the processing?[61] and
3) who benefits from the processing? [62]

The third question came into existence following the *Wirtschaftsakademie* ruling, whereof benefiting from the processing activity was held to add weight in the assessment of controllership.[63]

Any actor initiating or about to take part in a processing activity of personal data should assess on a case-by-case basis whether he is, by fact, determining the purposes and means.

'Purpose' denotes the specified, legitimate and explicit outcome that is expected of the processing activity. This could for instance be analytics, statistics, or targeted behavioral advertising. 'Means' on the other hand denote how the outcome should be achieved.[64] However, deciding on some means does not necessarily invoke controllership. WP29 distinguishes between 'essential' and 'non-essential' means. Essential means give rise to controllership and entail for instance decisions regarding third-party access to the data, time frame for processing or the selection of what data to process. Non-essential means, which could be determined

---

[57] C-101/01 *Lindqvist* [2003] ECLI:EU:C:2003:596

[58] *Jehovan todistajat* (n 49) paras 68 and 69

[59] Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (WP 169, 16 February 2010) at III.1.

[60] *Fashion ID* (n 50) para 76

[61] *ibid* (n 59) p 9

[62] European Data Protection Supervisor, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (7 November 2019) at 3.1.2

[63] *Wirtschaftsakademie* (n 48) para 40

[64] *ibid* (n 59) p 13

wholly or partly by the processor, would for instance concern the technical or organizational manners of processing the information.[65]

In determining whether a party is a controller or processor, the CJEU has also confirmed that access to the personal data being processed is not a prerequisite nor a requirement for controllership to arise.[66] Thus, if a party initiates a processing activity that he benefits from, he need not have access to the data processed to be considered a controller.

Each processing activity necessitates a separate evaluation of whether the party is a controller or processor. This means that a party can carry multiple roles at the same time, but for different processing activities. This is very important in terms of what obligations rest on the parties with each respective activity. In *Fashion ID* the CJEU stated in relation to controllership that a party is only responsible for complying with his role as a controller and the corresponding obligations in relation to the specific part of the processing where he determines the means and purposes.[67] Thus, for any subsequent processing or operations where he is not deemed a controller, any controller obligations and responsibilities cease to exist.

3.3 Introducing joint controllership

The concept of joint control did not exist under the DPD and is thus an invention under the GDPR. The addition of a new role under the instrument was founded on the increased complexity of determining traditional controller-processor roles, realizing that several parties may be involved in deciding upon the purposes and means of the processing.[68]

Joint control implies the multitude of controllers jointly determining the purposes and means of a processing activity.[69] The notion of 'joint' should be interpreted as "together with" or "not alone", implying some collective effort in the determination.[70]

Looking back at the definition of a controller it is, by text, quite broad. In *Google Spain* the CJEU nonetheless emphasized that 'controller' should not be interpreted restrictively, and that its objective is to ensure "*effective and complete protection of data subjects*".[71] This confirms

[65] WP29 Opinion 1/2010 (n 59) p 14
[66] *Jehovan todistajat* (n 49) para 69; *Wirtschaftsakademie* (n 48) para 38
[67] *Fashion ID* (n 50) para 74
[68] WP29 Opinion 1/2010 (n 59) p 18
[69] GDPR art 4(7), cf. art 26(1)
[70] WP29 Opinion 1/2010 (n 59) p 18
[71] C-131/12 *Google Spain and Google* [2012] ECLI:EU:C:2014:317 para 34

that the threshold for controllership to arise is not particularly high. This statement has since been offered repeatedly in following case law.

In lieu with the broad parameters for determining controllership set out in subchapter 3.2, this has resulted in an increase of situations in which two controllers jointly determining the purposes and means may exist.

3.4 Plausibility of joint control for third-party tracking cookies

While the CJEU has not expressly stated that third-party tracking cookies invoke joint controllership in general, recent case law, guidelines from certain national data protection authorities ("**DPAs**") and from the EDPS and WP29 speak in favor of this interpretation.

To assess the situation, we will first compare the key traits of tracking cookie placement with the defining elements for establishing controllership from subchapter 3.2. The placement of third-party tracking cookies usually entails the following elements:

a) It is the third-party that places the cookie;
b) it is often for the benefit of both parties, through either exposure, service improvement or payment;
c) the website operator cannot usually access the personal data stored by the cookie, although in the case of statistics or analytics he may have access to anonymized data-based on the personal data collected by the cookie;
d) the website operator sometimes can define certain parameters for what data is to be collected, to influence the statistics he receives;

The first question is whether the placement of tracking cookies may give rise to controllership. This would require 'placement' to constitute an act of 'determining' the purposes and means, jointly with a third party. In *Jehovah's Witnesses*, the CJEU established that 'determining' includes the ability to exert influence over the purposes and means of a processing activity.[72] In *Fashion ID*, decisive influence over the collection and transmission of personal data by embedding a social plugin constituted 'determining'. Now, embedding a social plugin has a similar outcome as the placement of cookies; their presence on a website initiates the collection and transmission of the personal data. One may therefore ask whether it is reasonable to presume that the placement of third-party tracking cookies would be considered 'decisive influence'. This is a probable outcome. Had the plugin not initiated any processing of visitors' personal data, there would be no case and certainly no need for the court to discuss the element of 'decisive influence' over the collection and transmission of such data anyways.

[72] *Jehovan todistajat* (n 49) para 40

Granted also that European Data Protection account for a technology neutral language, i.e. cookies and similar technologies, it is reasonable to presume that this ruling applies to similar technologies producing an equivalent outcome. Thus, the placement of third-party tracking cookies may constitute an act of 'determining' the purposes and means jointly with another.

The second is whether the fact that the third-party tracking cookie placement includes a benefit for the website operator is inducive of controllership. The court answered in the affirmative in both *Wirtschaftsakademie* and *Fashion ID*. In *Wirtschaftsakademie*, this was only established in the context of using the platform of Facebook to benefit from its associated services (i.e. analytics/statistics, where the website operator can toggle what data to be processed to provide such services).[73] Yet, in that case other elements played in on the establishment of joint controllership. Beyond the benefit Wirtschaftsakademie gained from this function, Facebook gained a benefit in return because the data collected by the cookies placed, whereof Wirtschaftsakademie could decide on the parameters of what data was collected, were also used by Facebook to improve their advertising system.[74] Benefit as a stand-alone element in this case and in the context of analytics/statistics was not inducive of joint controllership, but controllership. Thus, it is the existence of *mutual benefit* that may give rise to joint controllership. In *Fashion ID* mutual benefit was expressly recognized to give rise to joint controllership where the benefit for embedding social plugins entailed a commercial advantage or an increased publicity of goods, and the processing operation was performed in the economic interest of both parties.[75] According to the court, this was indicative of determining the 'purposes' of the processing jointly together. To conclude on this point, benefit by itself may be indicative of controllership, whereas mutual benefit is indicative of joint controllership. The result is that not all websites benefitting from placing third-party tracking cookies invoke joint controllership, depending on whether the third party also achieves some form of benefit. We will explore the meaning of this for different types of cookies in subchapter 3.5.

The third question is whether a website operator can be a joint controller even if it does not have access to the personal data processed by the third-party cookies it places. This has been affirmed in all the courts' cases dealing with joint controllership. In the context of cookies, the rationale is that a mere visit to the website may trigger the processing of personal data through such cookies. This may relate to the first question, namely that it is the website operator that initiates the processing by placing such cookies. Initiation is *de facto* indicative of controllership according to the WP29 and EDPS. Where a party does not initiate the processing activity or exert influence in determining the purposes and means, the lack of access to the data may

[73] *Wirtschaftsakademie* (n 48) para 40

[74] *Ibid* para 33

[75] *Fashion ID* (n 50) para 80

suggest no controllership. Yet, for third-party cookie placement, where initiation or the exertion of influence is inevitable, this appears to render the question of access irrelevant to the assessment of joint control.

The fourth question relates in large parts to analytics and statistics cookies. Does the ability to define the parameters for what data is to be collected indicate joint control? The answer is no. But it is indicative of control. According to *Wirtschaftsakademie*, the ability to toggle these parameters equals contributing to the processing of personal data. Even if the statistics are anonymous when the website receives them, the initial data collection consist of personal data. This fulfils the element of 'exerting influence' on the purposes and means of processing. This supports WP29 and EDPS findings, in that deciding on what data to be processed forms part of the 'essential means', which only a controller can decide upon. Thus, these findings are indicative only of sole controllership, and not joint controllership. Joint controllership requires a collective effort. If a website operator uses third-party tracking cookies and solely decide on (a) whether to place these cookies to receive statistics, (b) on the parameters for what data is to be collected and (c) the third party does not benefit from the processing activity in question, it would be difficult to argue that joint control exists.

Prior to the recent case law illuminating the defining elements of controllership, the view that third-party tracking cookies could invoke joint control had little support in both the legal text, guidelines, practice or academia. The odd example out might be that presented by WP29 in 2010, when they stated that "*ad networks and website operators are often joint controllers, as they jointly determine the purposes and means of the processing.*".[76] Following the assessment above based on today's criteria for controllership, joint controllership is highly likely for at least some types of third-party tracking cookies, if not all.

An interesting argument against the plausibility of joint control, is that there are doubts as to whether it was the intention of the CJEU to permit such a broad interpretation of joint controllership. Advocate General Bobek warned the court against adopting a too broad interpretation of joint control in *Fashion ID*, as a failure to create clear limits to the concept would render it difficult to assess who is ever "*not a joint controller*".[77] While the ruling followed the precedence of *Jehovah's Witnesses* and *Wirtschaftsakademie*, it left us with that exact question. Joint controllership was broadened, but any delimiting circumstances or elements were not discussed. Now, it may appear that the mere placement of third-party tracking cookies equates to determining the essential means, which in and of itself implies joint controllership for web-

[76] WP29 Opinion 2/2010 (n 8) p 11

[77] C-40/17 *Fashion ID* [2019] Opinion of AG Bobek ECLI:EU:C:2017:796 paras 71-72

site operators. It is highly regrettable that the court did not attach any strings to this argument. In academia, some argue that the ruling does not present an excessive broadening of the concept. Researcher Vrabec contends that this case only signifies joint controllership in the specific situation of embedding the Facebook "like" button.[78] Yet, as discussed under question one above, third-party tracking cookies produce an equivalent outcome to social plugins. We should therefore be careful of considering the ruling as isolated to only social plugins. Irrespective of the courts' intention, it is plausible that all third-party tracking cookie placement now invoke joint control.

The review above is only indicative of what may be to come. Until it becomes common practice (e.g. guidelines by EDPS, EDPB or several DPAs) or is affirmed by the CJEU itself, one cannot claim it as a certainty. Some DPAs have already started accounting for a broadened interpretation of joint controllership for such cookies. The ICO has for instance incorporated the ruling of CJEU in *Wirtschaftsakademie* in their guidelines, however only mention the factual circumstances that occurred in that case.[79] It does not elaborate on any other instances where joint controllership may occur for cookies. CNIL has also confirmed the plausibility of joint control when discussing the use of trackers involving advertising agencies but does not illustrate when joint control occurs.[80] The absence of any clear guidance at member state level may be due to the court's ambiguous precedence.

The result is that current case law and guidelines can neither confirm nor disconfirm joint control for *all* third-party tracking cookies. But it is reasonable to presume that at least some types of tracking cookies may invoke joint control. This flows from reading the three judgments together where certain key elements are repeated, in particular that of mutual benefit. It is more uncertain whether placement in and of itself will invoke joint control, as the CJEU has not had a chance to elaborate on this argument from *Fashion ID*. Website operators should nonetheless be cautious of this judgment, as we await a final verdict.

---

[78] Helena U. Vrabec, 'News from «cookie land»' (Leiden law blog, 8 August 2019) <https://leidenlawblog.nl/articles/news-from-cookie-land> accessed 19 September 2019

[79] Information Commissioner's Office, 'Guidance on the use of cookies and similar technologies' <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-else-do-we-need-to-consider/> accessed 22 November 2019

[80] Commission nationale de l'informatique et des libertés, 'Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif)' (4 July 2019) article 3 <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337> accessed 7 November 2019

3.5 Which third-party tracking cookies would invoke joint controllership?

If we consider that the placement in and of itself is indicative of joint controllership, all third-party tracking cookies would invoke joint controllership. However, if the court ruling was not intended to be interpreted this broadly, we may explore which cookies would more certainly fulfill the threshold. Reference is had to the cookie types set out in subchapter 1.3.2. Here, we described the different cookies that are for the purposes of (a) analytics/statistics, (b) advertising and (c) social plugins. As social plugins have already been ruled to invoke joint controllership in *Fashion ID*, only scenarios (a) and (b) will be assessed.

3.5.1 Third-party tracking cookies for the purpose of analytics/statistics

For such cookies, the website operator embeds analytical cookies belonging to an online service provider not associated with its own domain (a third party), for the purpose of receiving insight into for instance site traffic, content engagement of users, demographics or duration of visits.

Commonly the website operator can toggle what data the statistics should be based upon himself. This means he exerts influence on the essential means of the processing activity, which is indicative of controllership. This rings true to the traditional interpretation of controller/processor roles for these types of cookies. But two scenarios can arise here, whereof one can tilt the relationship into joint control; if the website operator is the sole benefactor of using these statistics, he is a sole controller. If both the website operator and the third-party benefit from the processing activity, they are joint controllers.

For website operators to be sole benefactors, the third party cannot have any benefit from the processing activity, such as an economic interest (i.e. increased publicity or commercial advantage) or other advantage (e.g. third-party improving its service or advertising service). It is important to note here that any such benefit must stem from *the processing activity*. If the data processing is directly used to improve the provision of the service or advertising service, this is a benefit for the third-party. Other benefits, such as monetary compensation for *providing the service*, does not equate to benefitting from the specific processing activity. Surely that can assist the third-party in investing more resources to improve his service, but it does not use the data processing activity to achieve such benefit.

The prime example is the situation referred to in *Wirtschaftsakademie*, where both the fan page creator (e.g. a website who creates a fan page) and Facebook are joint controllers as (a) the website toggles the data to be collected and (b) Facebook benefits from the processing as it uses the data to improve its advertising services.

For other, less obvious examples, we can peak into the interesting case of Google Analytics or Google Analytics 360, where Google deems the website operator a controller and itself a processor.[81] The first is a free service, whereas the latter is a paid service offered to website operators. Neither service give rise to a mutual benefit and subsequently joint control, IFF Google does not use the data collected through the processing activity to improve its services or advertising services. Initially, Google provides that it only uses the data obtained from such cookies to provide analytics to its customers (i.e. website operators).[82] If we take this as a given truth, there is no benefit for Google. However, customers may decide how the data collected via Analytics cookies is accessed and used by Google in their data sharing settings.[83] Furthermore, customers can link the analytics service with other services, such as Google advertising services. This entails that certain data collected by the Analytics cookie is accessed and exported to the linked service.[84] Google's use of these data in the linked service may be different from that in the initial processing for analytics purposes.

If such data sharing or linking of services renders the processing activity a benefit for Google, such as service or advertising service improvement, this could invoke joint controllership for the placement of Google Analytics cookies. Assessing whether that is the case would depend on the specific customer relationship with Google and Google's practices itself, which would entail a much more thorough analysis than can be covered in this thesis. This example thus serves to merely exemplify scenarios in which joint control *could* arise for analytics/statistics cookies.

3.5.2 Third-party tracking cookies for advertising purposes

For these cookies, the website operator lends advertisement space on its site to a third-party and places its tracking cookies to be provide relevant ads. As mentioned, this often involves adtech and RTB, whereof the website operator, third-party (service provider, usually providing an Ad Exchange) and other third-parties (advertisers, or ad networks) are remunerated. Prime examples are Google's AdSense or Yahoo Bing Network's Media.net, where the website operator partners up with either one of them.

In these instances, the website operator has no access to the personal data collected by the cookie and can usually not toggle any parameters for what data is to be collected. In the case

---

[81] Google, 'Data Processing Amendment to the Google Analytics Agreement' (9 September 2016) https://www.google.com/analytics/terms/dpa/dataprocessingamendment_20160909.html accessed 26 November 2019

[82] Google, 'Safeguarding your data: What is the data used for?' (2019) <https://support.google.com/analytics/answer/6004245> accessed 14 November 2019

[83] *Ibid* at 'data sharing'

[84] *Ibid* at 'product linking summary'

of Google, the information gathered is determined by its Authorized Buyers Real Time Bidding Protocol.[85] As established, non-access is irrelevant for assessing controllership. The ability to determine what information is collected is indicative of controllership on behalf of the third-party, whereas that is not the case for the website operator stripped of that opportunity.

If, and only if, the placement of these cookies is not deemed decisive influence invoking joint controllership, the assessment must come down to whether the website operator achieves any benefit from the processing activity. This may be a commercial advantage or economic interest.

The information collected from the cookies permits advertisers to present the visitor with highly relevant ads, if he wins the bid. In Google, the website operator is paid per impression and per click on the displayed ads.[86]

A bidding process naturally produce a higher price, which in return is converted to a higher profit for the website operator providing the ad space. It is documented that visitors are more likely to engage with ads relevant to them.[87] As a result, the profit return to website operators per-click may be increased. This provides an apparent benefit to website operators; however, the question remains whether this is a benefit resulting from the processing activity or the service in itself.

I argue that this is an economic benefit resulting from the processing activity. Firstly, while the bidding process itself may not be indicative of such benefit, it is based upon the information collected about the user. The advertisers' participation in the bid, and consequently the payment to the website operator, is solely based on these data. If the user's data were extracted from the equation, it would be less likely that certain advertisers would participate in the bid. Secondly, the provision of relevant ads based on the visitor's data increase the payment per-click to the website operator. Here, the website operator directly benefits from the processing activity.

Placing third-party tracking cookies collecting and sharing the information of users with other third parties for the purpose of a bidding process and increasing the relevancy of advertisings,

---

[85] Google, 'Authorized Buyers Real-Time Bidding Proto' (2019) <https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide> accessed 14 November 2019

[86] Google, 'AdSense revenue, How much will I earn with AdSense?' (2019) <https://support.google.com/adsense/answer/9902> accessed 14 November 2019

[87] Ari Juels, 'Targeted Advertising … And Privacy Too' in David Naccache (ed), *Topics in Cryptology – CT-RSA 2001* (Springer-Verlag Berlin Heidelberg 2010) p 409

consequently increasing the revenue of the website operator, creates a mutual benefit for the parties. Therefore, website operators can be joint controllers when lending their advertising space to third-parties using adtech and RTB.

Having reviewed that several, if not all, third-party tracking cookies invoke joint controllership, we may now move to assess how this shift from pure controller-processor relations to joint controllership will affect the division of information obligations and liabilities under GDPR and ePD.

4 How joint controllership would affect the division of information obligations and liabilities of the parties

4.1 Information obligations under Directive 2002/58/EC and Regulation 2016/679/EC

4.1.1 Setting or accessing tracking cookies under Directive 2002/58/EC

The ePD only sets requirements to the setting and accessing of tracking cookies, or the "*storing of information, or the gaining of access to information, already stored in the terminal equipment*".[88] In the course of any such action, the party seeking to place the cookies must comply with two obligations: (a) the actor must obtain the users' consent (b) based on 'clear and comprehensive information' presented prior to consenting.[89] It is permitted under the instrument for the user's acceptance to a cookie to also entail the acceptance of subsequent readings of it,[90] i.e. the monitoring of the user's internet browsing.[91] Thus, each reading of the cookie does not require a new consent request.

This obligation rest solely with the party seeking to set the cookies. For the placement of third-party tracking cookies this will always be the website operator. The instrument does not distinguish between – nor refer to – controllers or processors. Hence, in the overall assessment of who is a controller or processor for the purposes of the obligations under the GDPR, this obligation should be treated merely as a legal requirement.

Under article 4(11) of the GDPR, consent is defined as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes*", requiring either a statement or a 'clear affirmative action' on part of the user signaling his agreement.[92] The consent request must be provided clearly separated from other matter, in clear and plain language, and the

[88] ePD art 5(3)
[89] *Ibid*
[90] ePD recital 25
[91] WP29 Opinion 2/2010 (n 8) p 23
[92] GDPR art 4(11)

user must have the opportunity to withdraw his consent at a later time.[93] The specificity of the consent request entails that consent must be obtained for each separate purpose of processing for which the cookies are sought placed.[94]

The notion of 'clear and comprehensive information' to users relates to the principles of transparency, lawfulness and fairness of processing under art. 5 GDPR. In *Planet 49*, Advocate General Szpunar noted that the notion entails the ease for a user to determine the consequences of giving consent and that it is 'sufficiently detailed' for him to understand how the cookie functions.[95] The WP29 has provided a list of what it considers 'minimum requirements' to comply with this obligation but notes, harmoniously with the court in *Planet 49*, that this may vary depending on the case at hand.

If a website operator sets third-party cookies, he must at least inform of (a) the third-party's identity, (b) the purpose of processing, (c) what data is collected and why, (d) consent withdrawal information, and other relevant information if (e) the data is to be used for automated decision-making and/or (f) there is a risk of data transfers where no adequacy decision is in place.[96] The *Planet49* ruling also provided that the expiration date of the cookies and any third-party sharing, including their identity, must be informed of when setting advertising cookies to "*guarantee fair processing*". [97] The information must be presented using clear and plain language understandable to the average person, and the format in which it is presented is up to the website operator. Accessibility and clarity of the information must nonetheless be accounted for when choosing the format.[98]

4.1.2 Processing personal data under Regulation 2016/679

When tracking cookies invoke the applicability of the GDPR, another set of information obligations apply. In contrast with ePD, these rest with either the controller or the processor. The information obligations we will review relate to the lawful basis and the collection of personal data.

To start off, it is important to note that GDPR provide a list of principles for processing in article 5, which underpin all the obligations arising from GDPR. The responsibility for com-

---

[93] GDPR art 7

[94] GDPR recital 43; Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP259 rev.0, 10 April 2018) p 10

[95] C-673/17 *Planet 49* [2019] Opinion of AG Szpunar, ECLI:EU:C:2019:246 para. 115

[96] WP29 Guidelines on consent (n 94) p 14

[97] *Planet 49* (n 51) paras 76-80

[98] WP29 Guidelines on consent (n 94) p 14

plying with these rests solely with the controller.[99] These concern (a) the lawfulness, transparency and fairness of processing; (b) purpose limitation (i.e. processing only what is necessary for the specified purpose); (c) data minimization (i.e. not processing any unnecessary data for the specified purpose); (d) accuracy (i.e. correctness and quality of data processed); (e) storage limitation (i.e. not process for longer than necessary); and (f) integrity and confidentiality (i.e. ensuring the security of the processing activity).[100]

4.1.2.1 Lawful basis – which is permitted for third-party tracking cookies?

In subchapter 2.1.3 we saw that any placement of cookies invoking the applicability of GDPR must both ensure the lawful basis of consent under ePD and another lawful basis under GDPR. Article 6 GDPR sets out a list of lawful bases for when a processing activity is permitted, and the information obligations may vary depending on what basis is pursued. The article itself does not mention whether it is to be obtained by the controller or processor, but the principles under article 5 place the obligation to ensure the lawfulness of processing with the controller.

Tracking cookies process personal data for purposes of statistics/analytics and targeted advertising based on profiling/behavioral monitoring. The legal bases one could consider in this regard are (i) necessity for the performance of a contract, (ii) legitimate interest of the controller or a third party or (iii) consent.

Concerning the necessity to perform a contract, this requires the abovementioned purposes to be *necessary* to perform a contract. This would imply that it is indispensable for a user to access or use the website or shop goods. However, WP29 and EDPB have held that these purposes cannot be based on this basis.[101] The rationale is that the delivery of a service would never necessitate analytics, profiling or targeted ads. The argument that ads are necessary because they indirectly fund a freely accessible service or that analytics/statistics improve the service, has also been explicitly rejected.[102]

In the case of legitimate interest, the controller must have a stake or benefit from the processing, which outweighs the interests or rights and freedoms of the data subject towards his

---

[99] GDPR art 5(2)

[100] GDPR art 5

[101] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP 219, 9 April 2014) p 17; European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (9 April 2019) p 13

[102] EDPB Guidelines 2/2019 (*ibid*) p 12-13

personal data.[103] This interest must be both real and lawful and requires a balancing act on the part of the controller. Yet, invoking this basis for the abovementioned purposes has been firmly rejected by WP29 and EDPB.[104] Legitimate interest is sometimes allowed in the context of profiling,[105] but WP29 argued that it would be difficult to justify legitimate interest for purposes of marketing or advertising due to the intrusive nature of the activity (i.e. tracking across several websites and/or devices).[106]

This leaves us with the basis of consent, which has already been elaborated in relation to ePD in subchapter 4.1.1. Under the ePD, we saw that consent was required to be obtained by the one setting the cookies, and not specifically a *controller* or *processor*. This is quite similar under the GDPR. The instrument does not place the obligation to obtain consent on any specific party, however it is the duty of the controller to *demonstrate* that valid consent to the processing activity was given.[107]

4.1.2.2 Information to be provided to the user

When placing tracking cookies, article 13 GDPR requires a set of information to be provided the user prior to the collection. This information must be provided in accordance with the framework provided in article 12 GDPR. Compared to the requirements to consent and clear and comprehensible information under article 5(3) ePD, the GDPR obligations are either identical or very similar.

Similar to what we saw under ePD, article 12 GDPR requires information to be presented in an easily accessible form using clear and plain language that is concise and intelligible. In practice, this type of information is commonly provided wholly or partly through a privacy policy or statement,[108] whereof the WP29 has favored a layered presentation.[109] What is distinct about article 12 is that it also imposes an obligation on the controller to facilitate the exercise of data subjects' rights. This means that he must implement the necessary means for users to exercise such rights and act upon all requests submitted.

---

[103] GDPR art 6(1)(f); WP29 Opinion 06/2014 (n 101) p 24

[104] EDPB Guidelines 2/2019 (n 101) p 13; WP29 Opinion 06/2014 (n 101) pp 17-18

[105] GDPR recital 47; Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP251rev.01, 3 October 2017) p 14

[106] WP29 Guidelines on automated decision-making (*ibid*) p 15

[107] GDPR art 7

[108] Mike Hintze, 'In Defense of the Long Privacy Statement' (2017) vol 76 issue Maryland Law Review 4 p 1052

[109] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP260rev.01, 29 Nov 2017) p 19

Concerning the required information to be provided, article 13 GDPR is a bit more elaborative. Under ePD clear and comprehensible information was required for obtaining informed consent only and does not appear to invoke the entirety of the information obligations under the GDPR. As noted in *Planet 49*, only the information that is deemed necessary to understand the consequences of consent and the functions of the cookies would be required in that sense.[110]

Obligations	**Art. 13 GDPR**	**Art. 5(3) ePD**
Identity of controller, contact details and where applicable the controller's representative	X	X (only identity)
Contact details of Data Protection Officer, where applicable	X	-
Purpose of processing and legal basis	X	X
The recipients or categories of recipients of the personal data	X	X
Information must be provided if the controller intends to transfer PD to a third country and the existence or absence of an adequacy decision; or in the case of transfers referred to in art 46 and 47, or 49(1) GDPR, reference to any appropriate or suitable safeguards and how to obtain a copy of these if not made available.	X	(only information about risk of transfer)
Period of storage of data, or criteria to determine period	X	X
Existence of right to request access, rectification, restriction of processing, or object to processing, or right to data portability	X	-
Existence of right to withdraw consent	X	X
Right to lodge complaint with a supervisory authority	X	-
Existence of automated D, including profiling, and meaningful information about the logic involved as well as significance of envisaged consequences of such processing	X	X
If for other purposes, information on that other purpose prior to further processing.	X	-

Figure 1: Comparison of information duties under articles 5(3) ePD and 13 GDPR for tracking cookies.

Figure 1 sets out the information requirements under the respective provisions for comparative purposes. The relevance of comparing the two is to assess the extent of what duties may already exist on a website operator under ePD, irrespective of the controller-processor distinction under GDPR.

What we see is that the controller carries some additional duties under the GDPR. Firstly, he must provide the contact details of himself and his representative, where applicable, in addition to his identity. Granted that the controller has a data protection officer ("**DPO**"), he must

[110] *Planet 49* (n 51) para 77

inform of his contact details. Secondly, he must elaborate in greater detail the circumstances surrounding any third-country transfers as compared to under ePD. The same is true for the data subject's rights to request access, rectification, restriction of or objection to the processing, or data portability requests. Here, the controller must both inform of the existence of such rights and have the means in place to receive and act upon such requests.

The last two rights that separate the GDPR requirements from those under ePD are the rights to lodge a complaint with the SA and informing the users if another purpose of the processing is to be pursued, prior to such subsequent processing. This could for instance be if the controller wants to use the data collected for the purpose of targeting for new purposes, such as service improvement or statistics.

4.2 Liabilities under Directive 2002/58/EC and Regulation 2016/679

Article 15(2) ePD provide, as quoted by EDPB, that "*the provisions of [Chapter VII on remedies, liability and penalties] of [Regulation (EU) 2016/679] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.*"[111] Thus, only the provisions on liability and penalties under GDPR is applicable.

Under DPD, controllers were the only party who had strict liability towards data subjects.[112] Here, any fault on the processor's part would equate to liability only for the controller, even if the controller could prove he had an absence of fault in the supervision or choice of the processor.[113] This has changed under the GDPR, as the liability regime now applies to both controllers and processors.

Under chapter VIII, article 82 GDPR sets out the clauses for determining the liability of processors and controllers, and the right to compensation for data subjects. Any material or non-material damage resulting from non-compliance entitles the data subject to compensation from the controller or processor.

Examples of damages are for instance loss of control over personal data, limitation of rights, identity theft or significant economic or social disadvantages to the data subject.[114] While the

[111] ePD art 15(2), cf. EDPB Opinion 5/2019 (n 32) p 7

[112] Council Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 art 23

[113] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 J Intell Prop Info Tech & Elec Com L p 274

[114] GDPR recital 85

threshold for claiming such damages has not been elaborated in GDPR case law, it appears that it requires some sort of real-life impact on the data subject. Thus, for instance the inability to object to the placement of cookies or withdraw consent may not constitute 'damages', unless it bears real consequences for the data subject.

Like under DPD, controllers still carry a non-delegable duty of care under GDPR. Pursuant to article 82(2) GDPR, he shall be liable for any damage caused by the processing if that damage is a result of non-compliance with GDPR. This means that he still carries liability irrespective of whether the fault lies with the other controller(s) or processor(s) involved. The liability of processors, on the other hand, is limited to where it (a) has not complied with the specific processor obligations under GDPR or (b) has acted outside or contrary to the lawful instructions of the controller.[115] This signifies the different liability regimes applicable to controllers and processors.

Nonetheless, if several controllers or processors, or both the controller and processor are involved in the *same* processing and prove to *both* be responsible for the damages caused, both are liable for the entire damage.[116]

Exemptions from liability may apply if the controller or processor proves it is not 'in any way responsible for the event giving rise to the damage'.[117] GDPR does not give examples of how or when this exemption can be claimed. If we have recourse to the equivalent exemption clause under DPD, it may refer to "events beyond control", signifying an unusual event that cannot be avoided even by employing mitigating measures, and does not "*constitute the realization of the risk for which the person is strictly liable*".[118] The inclusion of the phrase 'in any way' suggests a strict reading of the exemption clause. From a contract law perspective, this closely resembles a strict force majeure clause– signifying a high threshold for exempting the party of any liability.

Beyond the liabilities for damages, national SAs has investigative and corrective powers under article 58 GDPR to remedy non-compliance against both controllers and processors. Amongst these powers, it is authorized to impose administrative fines under article 83 GDPR, either together with or instead of any such measures.[119]

---

[115] GDPR art 82(2)
[116] GDPR art 82(4)
[117] GDPR art 82(3)
[118] Van Alsenoy (n 113) p 283
[119] GDPR art 58(2)(i)

Article 83 GDPR sets two different sanction regimes: the first entails a fine up to 10 000 EUR or 2 % of the word-wide annual turnover, whichever is higher.[120] The other entails a fine up to 20 000 EUR or 4 % of the word-wide annual turnover, whichever is higher.[121] It is the latter regime that applies to the principles of processing, ensuring the lawful basis (and conditions for consent), provision of information and enabling the exercise of data subjects' rights. This regime therefore applies to the requirements to tracking cookie placement and use under both ePD and GDPR. Herein, the fines are not directed at the controller or processor *per se*.

It is mainly the controller who is responsible for the principles of processing under article 5 GDPR. The same is true for the ability to demonstrate and ensure consent, and for enabling the exercise of data subjects' rights. Under ePD, the website operator placing third-party tracking cookies carries some of the same duties in terms of obtaining consent and providing certain information to the data subject. Following article 15(2) ePD, this means that he may be liable for damages or penalties arising from articles 82-83 GDPR irrespective of whether he is a controller or processor. The question then becomes whether and to what extent a shift from controller-processor to joint controllership would impact the division of liability amongst the parties.

4.3 Comparing the required arrangements in controller-processor and joint controller relations

4.3.1 Requirements in controller-processor relations

For controller-processor relations, the mandatory content of their contractual agreement is set out in article 28(3) GDPR and include general clauses pertaining to the processing activity and the categories of data subjects and specific clauses pertaining to the processor's obligations.

Firstly, the general clause of a DPAg requires that the parties must at least set out (a) the subject-matter and duration of the processing; (b) the nature and purpose of the processing; (c) the type of personal data that is to be processed; (d) the categories of data subjects; and (e) the rights and obligations of the controller.[122]

Secondly, the DPAg must set out the specific obligations of the processor. Importantly, it is required that the processor only act on the documented instructions of the controller and is bound by confidentiality. Where the DPAg has set out instructions regarding the purposes and means, technical and organizational measures or requirements to data security, the processor

[120] GDPR art 83(4)
[121] GDPR art 83(5)
[122] GDPR art 28(3)

cannot deviate from these standards or pursue a different purpose of processing. His hands are tied by this contract, unless any act in question is in breach of member state or EU law. But even here he must first consult with the controller on this matter.[123]

Most relevant to the division of information obligations and liabilities is that the processor should assist the controller where possible, considering the nature of the processing, in fulfilling his obligation to respond to requests for exercising the data subject's rights.[124]

Article 28 does not give any further specifications regarding these two topics. However, the SAs and the European Commission can submit standard contractual clauses ("**SCC**") which further specify and clarify how the provisions are to be implemented.[125] No such clauses have yet been accepted, but in the future, these can prove useful as guidelines for what parties can or cannot do. The Danish SA was the first to submit an SCC proposal, but the EDPB rejected it.[126] In its reasoning, the EDPB nonetheless revealed some guiding points. It stated that:

"*If a paragraph specifying liability, governing law, jurisdiction or other terms is included, it cannot lead to any contradiction with the relevant provisions of the GDPR or undermine the level of protection offered by the GDPR or the contract*".[127]

This implies that the division of rights and obligations under the DPAg, such as information obligations, obtaining consent or liability, is possible if it does not contradict the instrument or minimize the level of protection it offers.

4.3.2 Requirements in joint controllership

In joint controller relationships, article 26 GDPR requires the parties to enter into an arrangement setting out "*their respective responsibilities for compliance with the obligations under [the GDPR], in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14*".[128] Contrary to what we saw in controller-processor relationships, this arrangement need not be manifested by a contract or other legal act, nor does it need to be publicized. However, the essence of the agreement should be available to the data subjects.

---

[123] GDPR art 28(3)(h)

[124] GDPR art 28(3)(e)

[125] GDPR art 28(7)-(8), cf arts 93(2) and 63

[126] European Data Protection Board, 'Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)' (9 July 2019) at 52

[127] *Ibid* at 47

[128] GDPR art 26(1)

The purpose of the arrangement is to clearly allocate the role and responsibility of each joint controller towards the user, and is deemed necessary to protect the rights of data subjects and appropriately allocate liability of each party.[129] Compared to what we saw under a DPAg, there are few to none mandatory clauses concerned with how the parties divide their responsibilities. As the WP29 observed, joint controllers can flexibly distribute and allocate obligations and responsibilities, but such distribution must ensure full GDPR compliance and take into account the factual circumstances.[130] The division must to some extent reflect the reality, i.e. who factually carries what obligations and responsibilities. In support of this view, a rule of thumb is that the parties should consider the risks each party is exposed to when drawing up the agreement.[131] Irrespective of the allocation the data subjects should be able to exercise their rights against both controllers.[132]

4.4 How a shift affects the division of responsibilities and liabilities

4.4.1 Principles of processing

Lindqvist noted that, although the principles of processing belong to controllers, the accountability principle can be included in the processing instructions of the DPAg.[133] Thus, in controller-processor relations, liability under article 5 may tilt to the processor in relation to the tasks or instructions specifically set out in the DPAg.

In joint controller arrangements, this would not look particularly different. Both controllers would *de jure* be obliged to observe the principles, in the context of their respective risks and responsibilities. But could one party impose that obligation solely on the other party? Such a division would be unlikely to succeed in practice. While the EDPB's guidance on SCCs concerned DPAgs, some points arguably apply to joint controller arrangement as well. Any term included cannot undermine the level of protection offered under GDPR. Read together with WP29 Opinion 1/2010, the division must reflect the circumstances as to who factually carries what risks and obligations in order to be GDPR compliant. In the context of third-party tracking cookies, it is also important to emphasize that joint controllership only exist for the parts

[129] GDPR recital 79

[130] WP29 Opinion 1/2010 (n 59) p 24

[131] Valentina Colcelli, 'Joint Controller Agreement under GDPR' in Ante Novokmet, Dunja Duic and Tunjica Petrasvevic (eds), *'EU and comparative law issues and challenges series'* (Faculty of Law, Josip Juraj Strossmayer University of Osijek 2019) p 1033

[132] GDPR art 26(3)

[133] Jenna Lindqvist, 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?' (2017) vol 26 issue 1 International Journal of Law and Information Technology p 58

where they jointly determine the purposes and means of processing.[134] This is generally held to be during the collection and transfer of personal data. In the case of third-party tracking cookies for RTB advertising, it is therefore impossible for the website operator to observe the principles of processing for any subsequent processing activity carried out solely by the RTB-provider and the participating advertisers.

4.4.2 Obtaining the lawful basis

In controller-processor relations, we saw that it may be possible to outsource the lawful basis to the processor in a DPAg, if it does not contradict GDPR or reduce the level of protection to data subjects. Website operators already have to obtain consent under ePD for third-party cookies. Requiring a double consent on both the website and the third-party site may severely disrupt the user's experience and cause 'information fatigue'. Thus, outsourcing this obligation to a website operator arguably strengthens the level of protection offered to the user. The WP29 and ICO supports the view that consent can be relied upon by other parties, if they are identified prior to obtaining consent.[135] Observing the general practice of third-parties and website operators, this also seem to be the standard approach. An example is Google' EU user consent policy, whereof the duty to obtain valid consent for any Google products embedded on the site rests with the website operator.[136]

In a shift to joint controllership, this point would likely not entail any change for website operators; ePD already place this duty on website operators and third-parties generally already rely on that consent.

However, one should emphasize that the consent given, either in controller-processor or joint controller arrangements, is only valid for the specific purpose informed of. A website operator acting as a joint controller is only *de facto* required to obtain lawful basis for the processing part in which he determines the purposes and means.[137]

The question then becomes whether article 28 GDPR permits the parties to shift the responsibility of acquiring a lawful basis for subsequent purposes on website operators. The article itself does not spoil whether it is possible. But similar counter arguments apply in this regard as it did for delegating the principles of processing. The website operator is only a joint con-

---

[134] *Fashion ID* (n 50) para 89

[135] WP29 Guidelines on consent (n 94) p 13; Information Commissioner's Office, 'Guide to the General Data Protection Regulation' (2019) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ accessed 22 November 2019

[136] Google, 'EU user consent policy' (2019) https://www.google.com/about/company/user-consent-policy/ accessed 22 November 2019

[137] *Fashion ID* (n 50) para 89

troller for the collection and transfer of the personal data, unless he gains a mutual benefit from the subsequent processing. The rule of thumb stipulated in 4.3.2 further requires the division to reflect the factual circumstances. The factual circumstances suggest that this responsibility falls with the third-party, as he is the one deciding on the subsequent purposes of processing and is the sole benefactor.

4.4.3 Information to be provided to the user

In DPAgs we saw that the information to be provided pursuant to article 12 GDPR is quite similar to that already imposed on website operators under article 5(3) ePD, and that at least parts of the controller's duties can be delegated to the processor. [138] In relation to data subjects' rights, the DPAg can lawfully stipulate the level of contact the processor must have with data subjects. Examples by EDPB include the use of standard answers to requests according to instructions given by the controller, forwarding requests or technical implementations facilitating the exercise of such requests.[139]

In a shift to joint controllership, the information to be provided would not significantly change unless the prior DPAg has not provided the above-mentioned instructions to the website operator.

Article 26(1) GDPR expressly provide that joint controllers should determine who is responsible for what in relation to the exercise of data subjects' rights and information to be provided. As ePD already impose a vast majority of the information duties on the website operator, it then comes down to who should (i) ensure data subjects' rights and (ii) provide elaborate information on third-party transfers.

As for the former point, a significant change follows from article 26(3) GDPR. Accordingly, data subjects can exercise their rights against both controllers. Thus, irrespective of who has the duty to execute requests under the arrangement, both parties must participate in the request procedure and do so within the appropriate timeframes. At the outset this may appear as a strenuous duty for any small-sized websites embedding third-party tracking cookies. However, like the solution offered under the DPAg, this could easily be resolved. If the third-party is the one carrying the duty of handling data subjects' requests, the website could incorporate a link to their request form or automatically forward any requests to that party. This would also be in line with the proposal in article 26(1) GDPR, stating that a contact point for the data subjects may be designated in the arrangement.

---

[138] EDPB Opinion 14/2019 (n 126) p 11

[139] *Ibid*

As for the latter point, the arrangement puts no boundaries on who should provide what information. Elaborate information on third-party transfers could therefore be delegated to the website operator. Yet, as flows from the guidelines of WP29 and CJEU case law, it may be more appropriate to impose that duty on the party naturally suited to inform of such matters. If the third-party is the one deciding upon the intentions of transfer and to what country, it may be more fitting that this information is given by him, in addition to any suitable safeguards and copies of such. That is not to say that he could also provide this information to the website operator for him to present to the website visitor, or that the website operator implements a link to the content on the third-party's site in its privacy policy.

4.4.4 Liabilities

Liability under both instruments arise from whatever obligations the party is placed with, either by virtue of article 5(3) ePD, or according to what is decided in the DPAg or joint controller arrangement under GDPR. As for breaches under ePD, the website operator will always be liable to pay compensation and fines under articles 82-83 GDPR. This liability can never be shifted.

As for breaches under GDPR, we saw that processors could only be liable for violating or acting contrary to the duties on processors or the lawful instructions of the controller.[140] In joint controller arrangements, the contractual liberty – and inherent responsibility – is fairly higher.

A big issue is that website operators usually have little negotiation power when entering into agreements with third-parties. Examples include the use of any Google or Facebook products including the placement of tracking cookies, where the website operator is merely presented a take-it-or-leave-it agreement. This may include unfavorable terms allocating certain responsibilities, or even clauses on liability caps. In a shift from controller-processor to joint controllership, the imposition of such terms may imply a bigger risk for website operators.

The prior subchapters have discussed whether certain obligations can be delegated to the other party in joint controller arrangements. It has mainly argued that, although the text does not put any strict limits on what can be divided amongst the parties, such division must consider the factual circumstances when allocating responsibilities and risk to avoid undermining the level of protection of GDPR. The questions left to discuss are what level of liability a website oper-

[140] GDPR art 82(2)

ators can have within such joint controller arrangement, and what the effects are of any contractual liability clauses.

4.4.4.1 Level of liability for joint controllers

In the case of compensation for damages under article 82, the controller is always be responsible for any damage resulting from a GDPR breach, unless the exemption clause applies.[141] This seems to suggest an equal level of liability amongst the joint controllers. However, article 82(5) GDPR states that the controller or processor paying the compensation is entitled to a sum from the other controllers or processors *only* corresponding to their responsibility for the damage.[142] While this only refers to the division of the compensation sum post-settlement, it is indicative of that different levels of liability apply according to the parties' responsibility.

In terms of the imposition of fines under article 83 GDPR, SAs are required to consider several circumstances under letters (a) to (k). As opposed to article 82(5), these circumstances do not account for different levels of responsibility amongst the roles. Recital 148 GDPR nonetheless reveals instances in which the administrative fines should be reduced for certain parties. These include cases of minor infringements, where the fine constitute a disproportionate burden on a natural person, the party's degree of responsibility, and "*any other aggravating or mitigating factor*".[143] Herein it also appears that GDPR breaches invoking the imposition of compensation claims or damages does not invoke joint and several liability for joint controllers where their responsibility is unequal.

Opinion 2/2010 by WP29 made an interesting argument that joint and several liability should be considered to eliminate uncertainties, but only where an allocation of responsibilities has not been contractually divided according to the factual circumstances.[144] This view cannot be deduced from either GDPR or any recent case law, which may indicate that this point of the opinion has been rejected.

Indeed, the recent rulings of the CJEU suggest that joint and several liability is rarely the case, as joint responsibility does not imply equal responsibility and the party's level of liability must be assessed with regard to all the circumstances at hand.[145] Unfortunately, in all cases the court has not illuminated *how* this affects the imposition of compensation sums or fines. In turn, the level of liability amongst joint controllers in the context of placing third-party track-

[141] *ibid*

[142] GDPR art 82(5)

[143] GDPR recital 148

[144] WP29 Opinion 1/2010 (n 59) p 24

[145] *Wirtschaftsakademie* (n 48) para 43; *Jehovan todistajat* (n 49) para 66; *Fashion ID* (n 50) para 70

ing cookies remains uncertain. While article 83 gives room for the SA to consider any contractual division of responsibility, article 82 does not mention any such mitigating circumstances for the national courts to consider. The absence of any guidance on this point is a missed opportunity to guide national courts and SAs in correctly assessing the division of responsibility in joint controllerships.

4.4.4.2 The effect of liability caps

Often arrangements include clauses either allocating or capping liability between the parties. It is uncertain how the contractual liability regime interplays with the statutory apportionment of liability under GDPR.[146]

Article 82 GDPR appears to follow the *ex turpi causa* doctrine, meaning that a co-controller cannot raise a claim against the other for his own misconduct (i.e. for conduct which he himself is responsible for).[147] If one party is sued for damages by a data subject under this article it is unlikely that the national court will consider any liability allocation clause when determining the compensation sum. But post-payment, the GDPR does not forbid any clause establishing the recovery of a certain sum or percentage to the other party. This view has been supported by the ICO, stating that the arrangement made is irrelevant when discussing damages, but that repayment from the other party is still possible.[148]

Article 83 GDPR provide a similar outcome. SAs are obliged to only consider the circumstances listed therein when imposing administrative fines. Thus, any limitation clause will not be effective when the fine is imposed, but there are no restriction for the parties to later recover a sum or percentage of the other.

In both instances this means that contractual liability clauses dealing with recovery post-payment are not regulated under GDPR.

A plausible reason for this silence is that the EU has not been awarded explicit competence by the member states to regulate contract law, and it must therefore approach any such issues

---

[146] Nick Pantlin and others, 'Supply chain arrangements: The ABC to GDPR Compliance – A spotlight on emerging market practice in supplier contracts in light of the GDPR' (2018) vol 34 issue 4 Computer Law & Security Review p 884

[147] DLA Piper, 'UK: Liability limits for GDPR in commercial contracts – the law and recent trends' (DLA Piper, 7 February 2019) https://blogs.dlapiper.com/privacymatters/uk-liability-limits-for-gdpr-in-commercial-contracts-the-law-and-recent-trends/ accessed 10 November 2019

[148] ICO (n 135) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/ accessed 27 November 2019

cautiously. However, the absence of any explicit competence does not hinder the EU from implicitly regulating some aspects of contract law. [149] Article 114 of the Treaty on the Functioning of the European Union ("**TFEU**") permits the EU to harmonize member states' laws when their divergence affects the smooth functioning of the internal market.[150] If liability caps in joint controller arrangements under article 26 GDPR is treated differently under member state law, the question therefore becomes whether this hinders the smooth functioning of the internal market. As the instrument is fairly new and there haven't been many cases touching upon this issue at member state level, this remains to be seen.

To conclude, a shift from controller-processor relations to joint controllership in the context of placing third-party tracking cookies would invoke a broader liability regime. However, website operators now deemed joint controllers would likely not carry equal responsibility for the processing activity. Regretfully, the defining perimeters for clearly assessing his level responsibility are sparse. In relation to the use of liability clauses in these arrangements, their effect depends on the contract law of the relevant member state. It remains to be seen whether this practice creates any divergence obstructing the smooth functioning of the internal market, in which case the EU will be competent to regulate the matter.

5 Conclusion

This thesis sought to explore whether and what third-party tracking cookies could invoke joint controllership, and how that would affect the division of the parties' information obligations and liabilities under ePD and GDPR.

By analyzing the defining elements of controllership, the thesis has shown that the placement of certain, if not all, third-party tracking cookies invokes joint controllership under GDPR. The ruling in *Fashion ID* indicated that the mere placement of cookies would invoke controllership. However, the CJEU has not clarified whether this interpretation is restricted to embedding social plugins or if other mitigating circumstances apply.

The consequence of the low threshold and uncertainty surrounding the defining elements of joint control is that website operators may be joint controllers without knowing it. This is an issue because website operators cannot foresee what actions invoke the responsibilities and liabilities attached to joint controllership. The fact that the EU advisory bodies and the court itself have not clarified the circumstances precluding or implying joint control in greater depth

[149] Manko, R., 'Contract law and the Digital Single Market: towards a new EU online consumer sales law?' (2015) PE 568.322 EPRS in-depth analysis p 5

[150] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2008] OJ C115/47 art 114

may also be a reason why national DPAs have been reluctant to touch upon this issue. In the near future, such clarification should be prioritized as it would simplify and harmonize the process for website operators and third-parties when determining their roles, and consequently increase GDPR compliance.

A shift from traditional controller-processor relations to joint controllership will affect the obligations of the parties towards visitors whose personal data is processed, but the extent of the impact will depend on the prior contractual arrangements between the parties. Some DPAgs already entail instructions to the processor regarding principles of processing, detailed information on third-party transfers and the exercise of data subjects' rights. For these parties the shift will not require any significant effort. For others, however, similar efforts should be considered to ensure compliance.

As for the impact of a shift on the division of liabilities, the ePD already holds website operators liable under articles 82-83 GDPR in respect of obtaining consent and providing information to the data subject. Thus, for these specific duties no change will occur. Under GDPR, articles 82-83 GDPR and CJEU case law suggest that an unequal level of involvement as controllers implies unequal responsibility, and that the liability of each party must be assessed on a case-by-case basis. However, neither the instrument nor the CJEU has illuminated what 'unequal responsibility' really means. In order to ensure the effective enforcement of GDPR on member state level and legal certainty for online actors, it is advisable that such guidance is provided.

As to the effectiveness of liability caps in joint controller arrangements, it is uncertain how a contractual liability regime interplays with the statutory liability regime under GDPR. Parties are free to incorporate clauses concerning recovery of damages or fines post-payment. Their effectiveness will therefore depend on the applicable member state law. It remains to be seen whether this practice creates any divergence obstructing the smooth functioning of the internal market, in which case the EU will have implicit competent to regulate the matter.

Table of reference

Table of cases

Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH (C-673/17) [2019] ECLI:EU:C:2019:801

Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH (C-673/17) [2019] Opinion of AG Szpunar ECLI:EU:C:2019:246

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17) [2019] ECLI:EU:C:2019:629

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17) [2019] Opinion of AG Bobek ECLI:EU:C:2017:796

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) [2014] ECLI:EU:C:2014:317

Lindqvist (C-101/01) ECLI:EU:C:2003:596

Patrick Breyer v Bundesrepublik Deutschland (C-582/14) [2016] ECLI:EU:2016:779

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SA-BAM) (C-70/10) [2011] ECLI:EU:C:2011:771

Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta (C-25/17) [2018] ECLI:EU:C:2018:551

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16) [2018] ECLI:EU:C:2018:388

Weltimmo s.r.o v Nemzeti Adatvédelmi és Információszabadság Hatóság (C-230/14) [2014] ECLI:EU:C:2015:639

Table of legislation

Consolidated versions of the the Treaty on the Functioning of the European Union (TFEU)

[2008] OJ C115/47

Council Directive (EC), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 pp 31–50

Council Directive (EC), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, pp 37–47

Council Directive (EC), Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. OJ L 321 pp 36–214

Council Regulation (EC), Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") OJ L 119, pp 1-88

Table of secondary resources

Article 29 Working Party, 'Opinion 1/2007 on the concept of personal data' (WP 136, 20 June 2013)

Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (WP 169, 16 February 2010)

Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' (WP 171, 22 June 2010)

Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2013)

Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP 219, 9 April 2014)

Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251, 3 October 2017)

Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP259 rev.0, 10 April 2018)

Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP260 rev.01, 29 November 2017)

Clarke, O., 'French CNIL issues new guidance on advertising cookies' (Osborne Clarke, 3 July 2017) https://marketinglaw.osborneclarke.com/advertising-regulation/french-cnil-issues-new-guidance-advertising-cookies/ accessed 9 November 2019

Commission nationale de l'informatique et des libertés, 'Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif)' (4 July 2019) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337 accessed 7 November 2019

Colcelli, V., 'Joint Controller Agreement under GDPR' in Ante Novokmet, Dunja Duic and Tunjica Petrasvevic (eds), *'EU and comparative law issues and challenges series'* (Faculty of Law, Josip Juraj Strossmayer University of Osijek 2019)

Council of the European Union, '9292/1/19 Rev 1: Note from the Presidency to the Delegations' (Brussels, 20 May 2019) https://www.politico.eu/wp-content/uploads/2019/05/Progress-report-v2-May.pdf accessed 9 November 2019

DLA Piper, 'UK: Liability limits for GDPR in commercial contracts – the law and recent trends' (DLA Piper, 7 February 2019) https://blogs.dlapiper.com/privacymatters/uk-liability-limits-for-gdpr-in-commercial-contracts-the-law-and-recent-trends/ accessed 10 November 2019

European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data

protection authorities' (12 March 2019)

European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' (16 November 2018)

European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (9 April 2019)

European Data Protection Board, 'Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)' (9 July 2019)

European Data Protection Supervisor, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (7 November 2019)

Englehardt, S., Narayanan, A., 'Online Tracking: A 1-million-site Measurement and Analysis' (2016) Princeton University https://chromium.woolyss.com/f/OpenWPM-1-million-site-tracking-measurement.pdf accessed 22 November 2019

Gomer, R. and others, 'Network Analysis of Third Party Tracking, User Exposure to Tracking Cookies through Search' (2013), vol 1 Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)

Google, 'About bidding on AdSense' (2019) https://support.google.com/adsense/answer/190436?hl=en&ref_topic=1628432 accessed 15 November 2019

Google, 'AdSense revenue, How much will I earn with AdSense?' (2019) https://support.google.com/adsense/answer/9902 accessed 14 November 2019

Google, 'Authorized Buyers Real-Time Bidding Proto' (2019) https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide accessed 14 November 2019

Google, 'EU user consent policy' (2019) https://www.google.com/about/company/user-consent-policy/ accessed 22 November 2019

Google, ‘Safeguarding your data: What is the data used for?’ (2019) https://support.google.com/analytics/answer/6004245 accessed 14 November 2019

Gordon, K., 'What is Big Data?' (2013) vol 55 issue 3 ITNow

Hintze, M., 'In Defense of the Long Privacy Statement' (2017) vol 76 issue 4 Maryland Law Review

Information Commissioner's Office, ‘Guidance on the use of cookies and similar technologies’ https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-else-do-we-need-to-consider/ accessed 22 November 2019

Information Commissioner's Office, 'Guide to the General Data Protection Regulation' (2019) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ accessed 22 November 2019

Information Commissioner's Office, ‘Update report into adtech and real time bidding’ (2019) https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf accessed 18 November 2019

Juels, A., ‘Targeted Advertising … And Privacy Too’ in David Naccache (ed), *Topics in Cryptology – CT-RSA 2001* (Springer-Verlag Berlin Heidelberg 2010)

Kristol, D. M., 'HTTP Cookies: Standards, Privacy and Politics' (2001) vol 1 issue 2 ACM Transactions on Internet Technology

Leiner, B. M., 'A Brief History of the Internet' (2009) vol 39 issue 5 ACM SIGCOMM Computer Communication Review

Lindqvist, J., ‘New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?’ (2017) vol 26 issue 1 International Journal of Law and Information Technology

Manko, R., 'Contract law and the Digital Single Market: towards a new EU online consumer sales law?' (2015) PE 568.322 EPRS in-depth analysis

Netscape.com, 'Persistent Client State HTTP Cookies' (curl.haxx.se) https://curl.haxx.se/rfc/cookie_spec.html accessed 22 November 2019

Pantlin, N. and others, 'Supply chain arrangements: The ABC to GDPR Compliance – A spotlight on emerging market practice in supplier contracts in light of the GDPR' (2018) vol 34 issue 4 Computer Law & Security Review

Raymond, E. S., *The New Hacker's Dictionary* (3rd edn, MIT Press 1996)

Schmücker, N., 'Web Tracking – SNET Seminar Paper Summer Term 2011' (2011) Berlin University of Technology http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.8976&rep=rep1&type=pdf accessed 22 November 2019

Van Alsenoy, B., 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 J Intell Prop Info Tech & Elec Com L

Voigt, B., Bussche, A., *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st ed, Springer 2017)

Vrabec, H. U., 'News from «cookie land»' (Leiden law blog, 8 August 2019) https://leidenlawblog.nl/articles/news-from-cookie-land accessed 19 September 2019

Wisman, T. H. A., 'Privacy, Data Protection and E-Commerce' in Lodder, A., Murray, D. (ed), *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing Limited 2017)