DATA SUBJECT REQUESTS

Working Paper 04/2018

IAB Europe
GDPR Implementation Working Group

Version 1.0
6 April 2018

About IAB Europe

IAB Europe is the voice of digital business and the leading European-level industry association for the interactive advertising ecosystem. Its mission is to promote the development of this innovative sector by shaping the regulatory environment, investing in research and education, and developing and facilitating the uptake of business standards.

About the GDPR Implementation Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector. The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

Acknowledgements

This working paper has been prepared by the members of the IAB Europe GDPR Implementation Group under the leadership of Noga Rosenthal, Chief Privacy Officer at *Epsilon/Conversant LLC*.

Contacts

Matthias Matthiesen (matthiesen@iabeurope.eu)
Director – Privacy & Public Policy, IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Public Policy Officer, IAB Europe

Contents

Overview

On 27 April 2016, the European Union adopted the General Data Protection Regulation ("GDPR").[1] GDPR will become directly applicable law in the European Union ("EU") and European Economic Area ("EEA") on 25 May 2018, superseding national data protection laws currently in place.

The GDPR will not only apply to companies based in the EU but also to companies all over the globe offering goods and services to people based in the territory of the Union, or monitoring the behaviour of individuals located within it. Data protection law regulates the processing of personal data, defined broadly as any information that relates to an identified or identifiable natural person, which may include, amongst others, online and device identifiers that can be used to single out a natural person, for example for digital advertising purposes.

GDPR grants data protection authorities the power to levy significant administrative fines against businesses found in breach of the law. Depending on the severity of the infringement, fines can reach up to €20,000,000 or 4 per cent of a company's annual global turnover – whichever is higher. Member states can also introduce additional criminal sanctions for breach of GDPR.

This document has been prepared by members of the IAB Europe GDPR Implementation Group (GIG) to provide guidance to companies across the globe on data subject rights.

Data Subject Requests

The GDPR expands and strengthens the existing data rights provided to data subjects under EU data protection law, as outlined in Chapter III of GDPR, Rights of the Data Subject. It also creates additional rights concerning "personal data" collected by or under the management of controllers. This data may in turn be processed by their service providers or processors.[2] Depending on the circumstances, data subjects may request to see their data held by the controller, request that the data be corrected or deleted, ask the data controller to cease or restrict processing of the data, and/or ask for the personal data to be ported over to another service provider.

A number of open questions have arisen around the digital marketing's compliance with these data rights. In particular, these data subject rights are challenging because these digital marketing

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter 'GDPR', available at http://eur-lex.europa.eu/eli/reg/2016/679/oj/.

[2] Controllers are directly affected by the rights afforded to data subjects under the GDPR. Organisations that act as processors are affected to a lesser degree, but should still be aware of these rights as they should be supporting the controller in responding to data subject requests. For instance, a processor may need to implement technological changes to enable the controller to comply with the data subject access rights. GIG recommends that both controllers and processors begin looking at their system to ensure that they have a policy and a process in place to properly respond to data subject rights.

companies traditionally hold pseudonymous data and do not always have direct relationships with individuals. For instance, a personal data touchpoint can be something as simple as a cookie identifier or mobile device ID.

The purpose of this document is to provide members of the digital marketing sector, including advertising technology companies, with an analysis of these rights and a better understanding of options on how to respond. This document will also provide companies with some basic compliance recommendations to review with their legal counsel to help them comply with these data subject rights.

It is crucial to emphasise that every technology platform in the digital marketing sector is unique, providing various services to its clients. Consequently, each company will implement processes and procedures that are particular to that company, resulting in different responses to data subject rights obligations. The intention of this document is to provide *general* guidance, thoughts, and options on how to comply with and respond to data subject rights. Companies should review this guidance, as it applies to their unique systems, with their legal counsel.

Further, interwoven into this document is the recommendation that companies take into consideration other data protection practices promulgated under GDPR. For instance, the principle of data minimisation requires that organisations should only process personal data to the extent necessary in order to achieve their processing purposes. Companies may consider taking further pseudonymisation or data aggregation steps, or even data deletion steps to comply with the data subject rights. Again, not all companies can undertake the same data minimisation, pseudonymisation, data aggregation or data erasure steps taken by other companies.

This document may be updated as more guidance is provided by regulators or due to feedback from IAB Europe members.

Step #1: Processor vs. Controller

One of the first steps that organisations in the digital advertising ecosystem need to undertake for compliance with these rights is to review GDPR itself and ensure that they understand how these rights affect their unique services and processes. In particular, digital marketing companies should first determine if they are a controller,[3] processor,[4] or joint-controller[5] or independent data controllers[6] in order to define which parties should be responding to the data subject.[7] Each distinction will pose different responsibilities in relation to the personal data they receive and process. IAB Europe's GDPR Implementation Group (GIG) will be providing guidance to members of

[3] Article 4(7) GDPR.
[4] Article 4(8) GDPR.
[5] Article 26 GDPR.
[6] Even if both companies are controllers does not necessarily mean that the companies are joint controllers. Instead, companies could be separate and independent controllers.
[7] Article 29 Working Party: 'Opinion 2/2010 on online behavioural advertising', adopted 22 June 2010, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf. The WP29 states in this document that "when behavioural advertising entails the processing of personal data, ad network providers also play the role of data controller."

IAB Europe about factors they may consider when determining if they are a controller, processor or joint-controller in a separate guidance document.

All organisations that act as a controller are likely to be directly affected by data subject rights. In turn, processors may need to help controllers handle these data subject rights. For instance, processors may need to implement technological changes that facilitate the controller's obligation under GDPR to respond to data subject rights.

Data processors should not reply directly to access requests, unless directed by the controller in a contract or otherwise. Controllers should expressly indicate each party's role in responding to data subject rights in their contract or data processing agreement/addendum. Unless directed by the controller, processors may not directly respond to a data subject access request or divulge the data subject's information without the controller's instructions. Doing so may be deemed a personal data breach, which includes an "*unauthorised disclosure of* […] *personal data*"[8] though the risk is minimized since the data is pseudonymized data (see the definition below). Further, a processor risks being deemed a controller if they begin responding to data subject rights requests without instructions or notification to the controller.

Step #2: Exception to Data Rights

The second step is determining whether digital marketing companies fall under one of the exceptions to responding to data subject rights. Under Article 11, if the controller processes personal data that does not require the identification of the data subject, the controller shall not be obligated to maintain, acquire, or process additional information in order to identify the data subject for the sole purpose of complying with GDPR[9]. Article 12 of GDPR also states that a controller may refuse "*to act on the request of a data subject for exercising his or her rights under Article 15 to 22*" if the controller "*demonstrates that it is not in the position to identify the data subject.*"

Most digital marketing companies collect, process and share pseudonymous data, which is personal data that cannot be attributed to a specific data subject without the use of additional information.[10] Such additional information may be kept separately, *"subject to the technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*[11] For instance, digital marketing companies traditionally collect and process identifiers, such as a cookie IDs or mobile device ID, or other pseudonymous information, which identify a browser or a device, and not an individual. They do not collect, receive or maintain personal information such as the name "John Smith."

In order to properly respond to a data subject right request, digital marketing companies would have to obtain additional information from a third-party company, such as a vendor, or the data

[8] Article 4(12) GDPR.
[9] Recital 64 of GDPR states that controllers use reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers." This leaves open the question as to what is reasonable in the pseudonymous context.
[10] Article 4(5) GDPR, definition of pseudonymisation.
[11] Ibid.

subject themselves, to identify and verify a particular individual based on the cookie ID or mobile device ID they hold. This additional data would be required to actually identify an individual.

> *In the example above, if an individual sends his name, e.g., John Smith, to an ad tech company, the ad tech company does not have such non-pseudonymised personal information on its system to provide information linked to the name. In this example, a controller would have to acquire and process additional information from a third party vendor in order to identify the data subject for the sole purpose of complying with GDPR.*

More concerning, how can digital marketing companies that rely on pseudonymous data *ever* confirm that the data belongs to the requestor? They are not in the position to directly identify the data subject and the personal data is not attributable to a specific data subject. Without the individual's name and address, how can digital marketing companies confirm that a cookie or mobile device ID is associated with a browser or mobile apps that belong to the individual making the data subject request even if the person supplies her name and address? Even with a name and address, digital marketing companies cannot tie that information to the pseudonymous data on their system.

An abusive husband, for instance, could submit his wife's laptop's cookie ID to a digital marketing company asking for access to the data tied to the cookie ID. The digital marketing company does not have the capability to verify that the cookie ID or mobile device ID belongs to the husband or the wife. The digital marketing company's actions could result in a personal data breach due to accidental or "*unauthorised disclosure of or access to,*" personal data of one person to another person.[12] It is nearly impossible for a digital marketing company to truly verify a person's ownership of a cookie ID or other identifier such as mobile device ID. The company could respond to the husband, for instance, with the wife's web browsing history.

The inability to verify that data belongs to the requestor begs the initial question: should digital marketing companies that only collect pseudonymous data respond to data subject right requests?

It is important for companies to evaluate whether they should respond to data subject rights, on a case-by-case basis, and document their reasoning. This analysis is crucial as European regulators have taken various positions on responding to data subject rights. For instance, the UK's Information Commissioner's Office (ICO) seems to bolster the view that subject access requests (SAR) must be responded to whenever possible. As stated in the ICO's 'Subject Access Code of Practice': "*the [Data Protection Act] places a high expectation on you to provide information in response to an SAR.*"[13] On the other hand, German regulators express caution in their short paper about data subject rights, recommending that companies consider other rights and freedoms, such

[12] Article 4(12), GDPR.

[13] UK Information Commissioner's Office: Subject Access Code of Practice Version 1.2, 6 September 2017, page 28, available at https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf.

as intellectual property rights and company secrets.[14] Other Data Protection Authorities have recommended that if a company is unable to verify the individual's identity, then it may look into providing the individual with information around how it creates its audience segments, but not necessarily provide the individual which the individual's particular segment.

Companies should review the options around responding to data subject rights with their outside counsel and determine whether to respond at all. **Once a determination has been made, it is strongly recommended that companies create an internal policy for responding to data subject rights, and also for all interactions with data subject access requests, particularly the reasons for denying such a request.**

Step #3: Policy

If a company determines that it has an obligation to respond to data subject rights requests, then we recommend that the company create. an internal, written policy around its data access response procedures. For instance, this policy should set forth which data subject identifiers (e.g., cookie ID's or mobile advertising ID's)[15] must be provided and the required verification information, as well as lay out the company's process for responding to such requests. In terms of process, companies should clearly state in writing that they are prepared to deal with a request, state the process for verifying or otherwise authenticating the ownership of the browser or device, enable searches to be run on the data subject identifier, and that the data can be located, reviewed and redacted if needed. The policy should also outline a retention period for maintaining the data subject's rights requests and company responses. In other words, if a data subject makes a request on 1 January 2019, how long will the company retain both the correspondence between the data subject and the company, and (as applicable) any output from the request?

Companies do not need to respond to data subject requests pertaining to data they have deleted, de-identified or anonymized, thus rendering it outside the scope of GDPR. Therefore, companies should consider implementing robust data retention policies not only to ensure compliance with GDPR but also to help limit the scope of their data access responses to data subject rights requests.

Email or Website

At the very least, a company should make publicly available an email address that individuals can use to make these requests. This email address may be the account used to contact the company's Data Protection Officer. Companies should consider taking steps to ensure that the email account is closely monitored, including during times the recipient or main person responding to such requests is on holiday or leaves the company. A company may also want to add a CAPTCHA or other

[14] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: *Informationspflichten bei Dritt- und Direkterhebung*, available at https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html.

[15] Examples of data subject identifiers include cookie identifiers and mobile device IDs.

mechanism to ensure that the requestor is a bona fide individual (e.g., privacy@company.com may be changed to email address Privacy AT Company .com).

A company may also have a website page that outlines its procedures for responding to data subject right requests. (See below for recommended steps for verification of data subject information). **At least one person should be responsible for responding to the data subject requests whether provided via the website, postal mail, email or the company's social media site.**

Verification of Data Subject Information

Upon receipt of a data subject success request, companies should take reasonable steps to confirm they have received a bona fide data subject right request to avoid processing a data subject request filed by an individual other than the authorized data subject. To mitigate against false claims, companies should verify the identity of the data subject, to ensure it does not "*adversely affect the rights and freedoms of others*."[16] This is particularly relevant for digital marketing companies which hold pseudonymous data.

It is also relevant where a single browser or device is shared by several individuals, resulting in a cookie ID being assigned to several individuals.[17] Further, an open question is how to respond to data subject right requests from an agent of a data subject. How does one verify that the agent has the right to request data subject requests of the individual? Companies may ask individuals to visit the companies' website and fill in a form to verify their identity and that the device ID was assigned to their device or access their website portal that verifies the device ID, pursuant to Article 12(6) GDPR.

It's important to note here that this verification process again raises a challenge for digital marketing companies. If a company maintains non-pseudonymised personal data, such as email addresses, it may send a verification link to the email account provided by the individual, ensuring that the data subject is the owner of that email address. There is no way for digital marketing companies holding only pseudonymised to verify the individual in this manner. However, despite not having the individual's name and address, there is potential that a digital marketing company should not refuse to provide data to the data subject and should instead attempt to verify the individual's right to the data, which includes taking reasonable steps at authenticating the data subject.[18]

Digital marketing companies which only process pseudonymous data should respond only to data subject requests tied to the identifier they use. These identifiers may include cookie IDs and mobile device IDs. If the data subject sends in her name, email address, or IP Address,[19] digital

[16] Article 15(4) GDPR.
[17] Alan Chapell: Is All Personal Data Equal Under the Law?, June 13, 2016, available at https://adexchanger.com/data-driven-thinking/personal-data-equal-law/.
[18] Recital 63 GDPR.
[19] If a data subject sends in their IP address, the working group recommends that the digital marketing company respond with a request for further information as IP addresses can be dynamic and they are more likely to be shared than cookie or mobile id's. Since this is not being used as an identifier and it is more likely to be shared by other data subjects, the working group determined that it is reasonable to ask the data subject

marketing companies should first request additional information from the data subject. This may include the actual cookie or mobile identifier[20] from the individual, which digital marketing companies are entitled to receive under Article 12(6) GDPR. If a data subject objects to providing the requested information, digital marketing may respond that they cannot complete the subject access request without first validating that the person making the request is entitled to receive the data.[21]

Also, if a website operator or mobile app provider (the first party) wishes to respond to a data subject right request that is tied to personal data held by digital marketing partners (the third party), it will need to point data subjects to its third party partners' site to fulfil such requests. For instance, if an individual went to a website and asked for access to her personal data collected by the website operator's partners, the website would not be able to reach out to its third party partners to request that the partner provide data on the individual. It could not, for instance, send the data subject's name and email address to the third party for the third party to look up that individual's information since the digital marketing company does not hold such identifiable data. Instead, the website operator should point the data subject to the digital marketing company's site where the company describes how it responds to data subject requests so that the company can ask for and verify via the identifier they use. Again, these identifiers may include cookie IDs and mobile device IDs.

Furthermore, once the data subject submits a request and provides an identifier, the digital marketing company could ask the data subject for a screenshot of the identifier to validate the request *or* the company could build a mechanism to automatically read the cookie from the individual's browser. If necessary, in the email requesting more information, digital marketing companies may (1) reference to Article 12(6), (2) explain how data subjects can locate their cookie or mobile identifier on their devices, and (3) remind the data subject that each browser will have a different set of cookies, and that the data subject's response will be tied to that particular browser. Again, the fear is that if the data subject refuses to provide the requested screenshot, companies cannot verify the authenticity of the request.

In addition to, or as an alternative, companies might request a declaration or affidavit from the data subject confirming that the data subject owns and operates the browser or mobile device and that the data subject has the right to make the data access request. If two people share a device or browser, then companies should consider having both individuals sign the affidavit or declaration.

While some companies may request copies of the data subject's government-issued identification paper for verification, digital marketing companies that do not typically collect non-pseudonymised personalized may not want to obtain and store such information, thereby subjecting themselves to more stringent data protection requirements tied to identifiable personal

for more information including asking the data subject to provide a mobile ID or cookie ID to help better pinpoint the data subject.

[20] Individuals may copy and paste their cookie ID from their browser or mobile device ID Google Android Device (which currently is accessible via their Menu>Settings>About Phone>Status. Individuals may also install a third party mobile app to obtain a mobile device id.

[21] Article 12(6) GDPR.

data. Further, there is no way to link the individual's name that appears on the identification to the cookie ID or other digital identifiers since these are rarely linked in the digital marketing world.

Again, digital marketing companies may explain their data subject right procedures and verification process on a page on their website. Companies may also use a data subject right form to help collect the information needed to process a data subject right request. However, companies cannot force a data subject to use this form.[22] Should companies receive a data subject request through some other channel, such as via an email or social media, they should refer the individual to their data subject right web page or ask the individual to contact the company via designated email (e.g., privacy@company.com).

In summary, because of the difficulty of verifying if a cookie or mobile ID truly belongs to the data subject requestor, and the fear of disclosing personal data to the wrong individual and thereby "adversely affect the rights and freedoms[23]" of another individual, companies should consider which of the following steps they will take once they receive a data subject rights request:

1. Recording and demonstrating that the company is not in a position to identify the data subject and informing the data subject that they will not respond to the request;[24]
2. Providing information[25] in its privacy notice or otherwise with instructions around how to responding to data subject rights requests, including the fact that a data subject must provide certain information, such as a screen shot of the relevant ID and/or requesting a declaration or affidavit that the ID belongs to the data subject, before the company will respond to the request; or
3. Creating a webpage that will enable a company to check the data subject's cookie on that browser and respond to the data subject rights request after the check.

Records

Digital marketing companies should maintain records of all data subject right requests they receive and all data access responses they issue, to demonstrate compliance. If a request is made via a website portal, companies may want to retain certain information for record keeping purposes to demonstrate compliance with data subject right request (e.g., cookie ID plus timestamp). This record may include the data subject request itself, the date of the request, the company's response (which may include a denial), the date of the response, along with a copy of the individual's identifier, proof of verification, and who handled the request. Companies may need to provide this information as evidence upon a supervisory authority inquiry. **In fact, companies should keep records of all correspondence with the individual concerned for a set retention period of 18-36 months at least.[26]** GIG members agreed that this data may be retained outside companies'

[22] UK Information Commissioner's Office: Subject Access Code of Practice Version 1.2, 6 September 2017, page 7, available at https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf.
[23] Article 15(4) GDPR.
[24] Article 11 GDPR.
[25] Article 12(1) GDPR.
[26] This retention period is based on unofficial feedback from Data Protection Authorities.

standard retention periods for data retained for their services, as this is separate data, processed for separate purposes and under a different legal basis (compliance with the law).[27]

Training

Digital marketing companies must train their personnel to respond to these data subject right request, according to their policy. The internal policy should be readily available in a central location, such as the company's intranet. In the company's general data protection training, all staff members should be trained to recognise GDPR data subject right requests, even if the requests itself are not identified as such. For example, an individual may request to know what data the company is holding or using without mention of GDPR and without labelling her inquiry as a data subject right request. More detailed training on handling these data subject rights should be provided to relevant staff. Specifically, the marketing department, the data protection team, and the legal department will need more tailored training as they may be more involved in handling these requests. Companies should also provide a hierarchy to enable staff members to flag an issue to senior managers, should a data subject be dissatisfied with the initial data access response. The senior manager should then review the response and determine next steps.

Specific Data Subject Rights

Information

Data controllers must communicate transparently with data subjects about the processing of their personal data.[28] Such communications must be provided in a concise, transparent, intelligible, and easily accessible manner, using clear and plain language.[29] The controller must provide the data subject with the information outlined in Chapter III, Section 2, Articles 13-14 of GDPR. This document will not concentrate on this provision.[30]

Right of Access

Under GDPR, data subjects have the right to ask a data controller if it is processing their personal data.[31] Upon a data subject rights request, and subject to certain exceptions, the controller must

[27] Article 6(1)(c) GDPR.
[28] Article 13 GDPR.
[29] Further guidance around this requirement may be provided by IAB Europe. Readers may also view the Information Commissioner's Office guidance around Transparency for further guidance, https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.
[30] Under Article 15(2), where personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguard pursuant to Article 46 relating to that transfer. Meaning, the data subject should be informed if the Personal Data was transferred to a third country based on standard contractual clauses or Privacy Shield.
[31] Article 15 GDPR.

give the data subject the following information, which may be included in companies' privacy notice or other public facing document:[32]

1. Whether the subject's personal data is processed;
2. The purposes of processing;
3. The categories of data being processed;
4. The categories of recipients with whom data may be shared, in particular recipients in third countries (non-EU countries) or international organisations;[33]
5. The retention period;
6. The data subject's rights to rectify or erase personal data, and right to restrict or object to the processing of personal data;
7. The right to bring a complaint to a supervisory authority;
8. Information as to the source of the data, if not collected directly from the data subject;
9. Information about the existence of any *automated* processing, including profiling, referred to in Article 22(1) and (4) that has a significant effect on data subjects, along with the parameters of such automated decisions; and
10. A copy of the personal data being processed (if requested).

Copy of the personal data being processed

Controllers must disclose a copy of the personal data they process if requested by the data subject unless subject to certain exceptions.[34] It is important to understand that the personal data set disclosed to the data subject will vary by company. For instance, disclosure requirements will vary depending on whether the company is classified as a processor or a controller. A data processor, such as a technology platform, that receives a direct request should not disclose controller data unless instructed to do so by the controller.

Digital marketing companies could consider doing a "table-top exercise" before the GDPR goes into effect, testing what data they would divulge when they receive a request connected to a digital identifier. Also, since it is nearly impossible for companies to verify the identity of the data requestor, companies could consider not divulging raw data (e.g., browsing history or click stream data) to the requestor. Providing the data subject with their audience segments may be sufficient. This is because the consequences of having a personal data breach or violating the data protection rights of an individual outweighs the need to divulge such raw data to the requestor. It may also result in harming a company by revealing its trade secrets (see discussion below).

Automated Processing: Profiling?

[32] Article 13 GDPR.

[33] Under Article 15(2) GDPR, where personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguard pursuant to Article 46 relating to that transfer. Meaning, the data subject should be informed if the Personal Data was transferred to a third country based on standard contractual clauses or Privacy Shield.

[34] E.g., Article 15(4), the right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Under the GDPR, companies are also required to divulge information about the existence and parameters of any *automated* processing, including profiling, that has a significant effect on data subjects. "Profiling" is defined as

> *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*[35]

Profiling becomes relevant when its conclusions and categorizations trigger automated decision-making.

The Article 29 Data Protection Working Party (WP29) has published guidelines on the definitions of automated decision-making and profiling, as well as which decisions have a legal or "similarly significant" effect.[36] "Legal effects" are those that have an impact on an individual's legal rights such as having an effect on a person's legal status. Additionally, "significant effects" are those effects that are equivalent or similarly significant to legal effects. The Article 29 Data Protection Working Party expressly stated that typical interest-based advertising will not have a similarly significant effect,[37] as it is unlikely that an advertisement (which an individual can choose to ignore) will have a legal or significant effect on data subjects.

However, the Article 29 Data Protection Working Party did provide considerations to help digital marketing companies determine whether their business practices could have a significant effect on an individual, such as (a) the intrusiveness of the profiling process; (b) the expectations and wishes of the individual; (c) the way the advertisement is delivered; and (d) the particular vulnerabilities of the individuals served with relevant advertisements. For instance, the Article 29 Data Protection Working Party noted that price differential can have a significant effect on an individual.[38]

Digital marketing companies - and the websites and mobile applications they support - should be transparent about their business practices. At the very least, they should disclose if personalized advertising is occurring on their site, which technologies they use to deliver that advertising, that the data subject may opt-out at any time, and how the data subject may do so. They should also review the Article 29 Data Protection Working Party's guidance around when their actions may be bucketed into being considered "profiling."

Trade Secrets

The GDPR provides that no one individual's personal data access rights should adversely affect the rights or freedoms of the company or other individuals, including trade secrets or intellectual property, and in particular copyrights protecting software.[39] Companies are understandably

[35] Article 4(4) GDPR.
[36] Article 29 Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp 251 rev01).
[37] WP29 Profiling Guidelines (wp 251 rev01), p. 22.
[38] Ibid.
[39] Recital 64 GDPR.

concerned about revealing trade secrets when responding to a data subject access requests. Specifically, companies worry that a bad actor or competitor could reverse engineer trade secrets from data turned over pursuant to a data access or data portability requests. **Digital marketing companies should not provide data that may reveal trade secrets- e.g., if the release of the parameters of automated decision making would involve the release of trade secrets. However, though digital marketing companies can limit the scope of the data released if such release may harm the company or its intellectual property, they may not refuse to release any data at all. They should also document the logic behind why the release of such information would lead to a revelation of a trade secret.**

Refusal

Digital marketing companies must provide a valid reason for refusing to provide data to a data subject. For instance, if a digital marketing company is a processor or is unable to verify the individual's identity, then it must provide this reason to the data subject. It is important to note that the bar for refusing data access rights is high, as evidenced in the Dawson-Damer case.[40] It should be noted, though, that the Dawson-Damer case involved personal data that was identifiable to the individual. Further, as noted before, the German regulators have offered more leeway for refusals. Digital marketing companies also must inform individuals of their rights to lodge a complaint with the supervisory authority and seek judicial relief.

Method of Transfer

Digital marketing companies should also have a method to 'transfer' or provide access to the data in response to any data subject access requests. GDPR states that, where possible, "*the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data*."[41] Therefore, digital marketing companies might consider developing or implementing systems to provide data subjects with remote access to the data held by that company, once the individual's identity is verified. Companies should work towards ensuring that this data is provided to the individual in a secure manner.

Fees

Under Article 12(5) of the GDPR, controllers may no longer charge a reasonable fee for responding to data subject requests. Article 12(5) states that "*information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 of GDPR shall be provided free of charge*." The initial copy of the data access response must be free of charge, but controllers

[40] The Dawson-Damer case is available here, http://www.bailii.org/ew/cases/EWCA/Civ/2017/74.html. For further discussion on this topic, please visit, "ICO guidance: a good re-SAR-It for controllers?" by Alexander de Gaye, http://privacylawblog.fieldfisher.com/2017/ico-guidance-a-good-re-sar-lt-for-controllers/.

[41] See, e.g., where the Federal Court of Germany clarified though a credit rating company needed to make credit scoring more transparent, it did not have to disclose its algorithm model in order to protect the credit reference agencies' trade secrets. Press release of the judgement available at http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2ef8cefa03b7d0493f54c1bc71ee0a53&anz=1&po s=0&nr=66583&linked=pm&Blank=1 (last accessed 28 February 2018).

may charge a reasonable fee for further copies.[42] For instance, if a data subject, or an intermediary on behalf of data subjects, makes multiple data access requests, then digital marketing companies can consider charging a reasonable fee, based on administrative costs, for any further copies requested. This means that an intermediary may be charged a fee if it makes multiple data subject requests on behalf of various individuals. **The data controller bears the burden of proof to show why a request is excessive, and thus necessitates a fee. Therefore, they should document the number of data subject's requests in order to demonstrate that they were excessive and burdensome.**

Timing

A controller must respond to the data subject requests iterated under Articles 15 to 22 without *"undue delay and in any event within one month of receipt of the request."*[43] If a request is too complex to address within one month, then this can be extended to three months. However, the controller shall inform the data subject of any such extension, and the reason for such delay, within one month of receipt of the request.[44] **Controllers should be mindful that they bear the burden of proving that a request is "complex," and digital marketing companies should document their arguments for concluding that this request warrants extended time.**

Again, digital marketing companies should consider maintaining records of any and all communications with data subjects, including exchanges beyond the initial request and response. These additional exchanges between the digital marketing companies and the data subject may cause discussions to extend beyond the one-month period. If they do, the digital marketing company's records would demonstrate that it needed additional, necessary information to respond to the data subject request and that the time for responding to the request did not run until the company received all the necessary information. **As stated before, the correspondence (and underlying personal data responses) with each data subject should be retained for a period of 18-24 months at least.**

Right to rectification

"*Taking into account the purposes of the processing,*" individuals have the right to require a controller to rectify any errors in its records of their personal data. Such corrections may include completing incomplete personal data where appropriate by means of a supplementary statement.[45] Companies should create a policy for the rectification process, which must include verifying the data subject's identity prior to making any changes.

Certain companies that create audience segments (e.g., website visitors that are interested in "Shoes") may be able to adjust a data subject's audience segment per a data subject request (e.g., switching the data subject's categorization from "Potentially visiting France" to "Homebody"). The

[42] Article 12(5) GDPR.
[43] Article 12(3) GDPR.
[44] Ibid.
[45] Article 16 GDPR.

resulting change may not be reflected until the digital marketing company encounters the data subject on another website.

Keeping data minimisation principles in mind, an alternative position is that digital marketing companies could implement their policy and procedures around the right of erasure (see Right of Erasure, below). To be clear, digital marketing companies may not be able to rectify the raw data underlying their audience segments, such as the recorded, underlying URLs or mobile device locations. These logs are simply a record of the sites or applications or latitude/longitude the data subject visited or even a record tied to advertisement itself instead of being tied to the individual's personal data (e.g., an ad was delivered to a site at a certain time of the day, an individual clicked on it, etc.). These data points are an accurate reflection of data collected by digital marketing companies.

Digital marketing companies may allow individuals to rectify their audience segments. However, many digital marketing companies create audience segments based on algorithms and correcting such segments could conflict with that algorithm. Additionally, digital marketing companies may find data rectification to be extremely complex or nearly impossible, as doing so could require the companies to obtain and correct information across various databases. Therefore, responding by erasing the data might be a more direct solution for the data subject, as they will no longer be 'wrongly' associated with an audience segment.

Right of Erasure

Data subjects have the right to erasure – which requires the controller to delete from its records all their personal data concerning the individual, without "undue delay" when *one* of the following conditions apply:[46]

1. *"the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;"*

The above condition means that digital marketing companies should review and create a general policy as to whether they need to retain certain data for the purposes for which it was originally collected or processed, such as billing, fraud prevention or other security reasons. If a company determines not to erase certain data, it must maintain clearly demonstrable records of its decision and continued processing needs, as data protection authorities will likely offer a very narrow interpretation of when it is truly necessary to retain data.

2. *"the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;"*

[46] Article 17(1) GDPR.

This provision applies to those digital marketing companies that are controllers relying on consent[47] as the legal basis for processing the data subject's personal data and data subjects subsequently withdraw their consent. The personal data is erased once data subjects withdraws their consent.[48] Controllers should also review whether there is another legal ground for processing the data (e.g., legitimate interest such as retaining the data for billing, to prevent fraud).

3. *"the data subject objects to the processing pursuant to Article 21(1) (right to object) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);"*

This provision applies to those digital marketing companies that are controllers relying on legitimate interest as the legal basis for processing the data subject's personal data.[49] When the data subject has objected to the processing, "*on grounds relating to his or her particular situation*,"[50] and also asks for their data to be deleted, a controller relying on legitimate interest can deny this request if it proves its interests outweigh the individual's rights. Companies could argue that the interest of preventing fraud, offering security services or maintaining data for financial records or reconciliation, may outweigh individual rights. Again, companies should document their logic if they determine that they need to retain certain data.

4. *"the personal data have been unlawfully processed;"*

This provision applies when the underlying legality of the processing is in question and therefore deemed unlawful. Personal data is processed unlawfully if the legal basis for processing is invalid or non-existent, but also if the processing does not comply with GDPR's principles of data processing.[51] Should the legal basis for processing be unlawful, a digital marketing company would have to delete the data at the data subject's request.[52]

IAB Europe's GIG interprets that companies may comply with this requirement by deleting or hashing (without the possibility of singling out a browser or device) the cookie ID (without the ability to decrypt the hashed information including throwing away the key), mobile ID or other identifier used to connect the user level data to the ID. The ID must be either deleted or hashed on the digital marketing company's database. A company may also then either delete the cookie on the individual's browser or adjust the expiration date of the existing cookie on the individual's device. A company can also tell data subjects how they may delete their cookies via browser controls. In the case of mobile apps, an individual should be advised to reset the mobile advertising id. Either

[47] To be clear, some companies may rely on consent for dropping cookies on an individual's browser. They may then rely on Legitimate Interest to process the personal data they collect using that cookie. For an excellent discussion on this topic, please see, "GDPR + e-Privacy = :-(" by Phil Lee.
[48] A revocation of consent is not the same as a request for deletion. Revocation is prospective, not retroactive. It results in the data controller and data processor no longer processing the personal data. Deletion is not necessary unless the data subject requests that the personal data be erased.
[49] Article 6(1)(f) GDPR.
[50] To be clear, Article (21)(1) of GDPR reflects that not every data subject objection triggers a company's obligation to start new legitimacy test- only objections which are based on concrete particular situation of data subjects.
[51] Article 5 (principles), Article 6 (legal bases) GDPR.
[52] Two further grounds for erasure exist under Article 17 (1)(e),(f), GDPR, but are unlikely to be invoked against online advertising technology companies.

way, the device ID becomes anonymized only when it is hashed on the server side (company side) AND deleted on the data subject's side.

Eliminating identifiers (and/or the ability to single out an individual) associated with the data, or by resetting a mobile ID, a company will effectively break the link between the personal data and an identifiable person, leading the digital marketing company to no longer have personal data – not even pseudonymised data. Instead, the company will hold anonymous data which falls outside the scope of GDPR. **This interpretation relies entirely on the company's ability to prove that there is no way to tie the data collected to any person, including no way of treating that individual differently (or a device which will be treated by data protection authorities as a proxy for the individual).**

Right to restriction of processing

The right to data restriction is a new data subject right. Data subjects may limit the purposes for which a controller can process their data.[53] This is an intermediary step short of deletion that individuals can request when they object to certain ways their data is processed (e.g., legal claim).

Data subjects have the right of data restriction when one of the following conditions applies:[54]

1. The data subject contested the accuracy of the collected personal data and the controller is in the process of verifying the accuracy of the personal data;
2. The processing is unlawful and the data subject opposes erasure of the data and requests restriction instead;
3. The controller no longer needs the personal data for the purposes of the processing but the data subject wants to maintain the data for the exercise or defence of legal claims; or
4. The data subject exercised the right to object pursuant to Article 21(1) and the controller is in the process of verifying whether its legitimate interests override the interests of the individual.

As a result of this right being introduced, data controllers should ensure that they have the ability to "pause" or suspend the processing on any restricted data. For instance, a digital marketing company may make selected data unavailable for further processing or flag the data on the servers to automatically exclude it from processing. Organisations may consider moving restricted data to another data system to prevent processing.

This requirement could also be fulfilled by offering data subjects an alternative opt-out. The digital marketing company could drop an opt-out cookie on the user's browser, or an equivalent mobile device ID opt-out, so that the digital marketing company would no longer collect any data, even for measurement or ad delivery or reporting purposes. This would flag the individual's browser or mobile device as restricted and would prohibit further data processing.

[53] Article 18(1) GDPR.
[54] Ibid.

In its response to a data subject right request, the digital marketing company should inform the data subject that even though their data is restricted and will no longer be processed in an active manner, it may still be stored. Internally, the organisation may also determine whether it has a reason to push for the data to be processed, despite the request (for example, if the organisation has proof of the data subject's consent).

If a controller has contractually disclosed personal data to a third party, and the data subject's data has since been restricted, the controller must notify those third parties of all changes. The controller shall also inform the data subject about those recipients if the data subject requests it. If the controller can prove that this obligation is impossible or would require a disproportionate effort, then there is an exemption under Article 19 for this obligation to notify the data subject and third party partners.

Personal data may be unrestricted and processed again, when one of the following conditions applies:[55]

1. if the individual has provided consent — he/she must be informed that the digital marketing company is processing the personal data again;
2. for the exercise or defence of legal claims;
3. for the protection of rights of another individual or organization; or
4. for reasons of important public interest of the EU or EU country.

Right to data portability

The right to data portability is also a new data subject right that requires more than the other data access rights.[56]

1. Data subjects have the right to receive the personal data **that they have provided** to a data controller if:
    a. the processing is based on *consent*,[57] or on a contract,[58] and
    b. the processing is carried out by automated means.
2. The data subject shall have the right to receive the personal data concerning him/her "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller."[59]
3. This right allows the individual to have the controller transmit or port the data to another controller.

Data portability rights are only triggered in a narrow set of circumstances.

First, as mentioned above, this right only applies if the individual provides the data to the controller. Individuals do not always provide data to controllers in the digital marketing ecosystem. For instances, digital marketing companies collect data from individuals as they visit digital properties,

[55] Article 18(2) GDPR.
[56] Article 20 GDPR.
[57] Article 6(1)(a), Article 9(2) GDPR.
[58] Article 6(1)(b) GDPR.
[59] Article 20(1) GDPR.

such as websites and mobile applications. Data portability applies only to data that has been provided to the controller by the individual in question, not data created by the company or provided to the company by others. It does not concern, for example:

1. Data provided by others about this individual;
2. Data produced by the controller; and
3. Data derived or inferred by the controller.

Thus, the term "provided by" includes personal data that relate to the data subject's activity or result from the observation of an individual's behaviour, but does not apply to any subsequent analysis or inferences of that behaviour. The Article 29 Data Protection Working Party agreed with this analysis, stating in its guidelines that data "provided by" the data subject including its "history of website usage" but not the subsequent data created by the controller such as a user profile.[60] Any personal data that have been generated by the data controller as part of the data processing (for example through a personalisation or recommendation process or user categorisation or profiling) are data that are **derived or inferred** from personal data provided by the data subject, and are not covered by the right to data portability.[61]

Second, data portability rights may be triggered if the legal basis for collecting the personal data is based on consent,[62] explicit consent,[63] or for the performance of a contract.[64] This right does not apply when processing is based on different legal bases than individual's consent or performance of a contract. For instance, some companies may rely on consent for dropping a cookie on an individual's device, per Article 5(3) the ePrivacy Directive, but rely on Legitimate Interest for processing of data collected via the cookie. Meaning, some companies may provide data subjects with a copy of their cookie under the requirement to port an individual's data because that is the only data that is obtained under consent.

Finally, the right to data portability cannot adversely affect the rights and freedoms of others (*e.g.,* when more than one individual is concerned).[65] When digital marketing companies cannot verify that an identifier belongs to the data subject, honouring a data portability request could result in releasing data to the wrong recipient, and thereby adversely affect the rights and freedoms of the true data subject. This could potentially also constitute a personal data breach though the harm is minimized since digital marketing companies are likely collecting and storing pseudonymized data. Therefore, companies should be cautious in responding to such data portability requests. **Again, if**

[60] Article 29 Data Protection Working Party: 'Guidelines on the right to Data Portability (WP242 rev.01)', page 9-10.For a summary of this data subject right, see: 'The Article 29 Working Party Issues Final Guidelines on the right to data portability,' https://www.twobirds.com/en/news/articles/2017/global/article-29-working-party-issues-final-guidelines-on-the-right-to-data-portability by Ruth Boardman, Ariane Mole and Gabe Maldoff.
[61] Ibid.
[62] Article 6(1)(a) GDPR.
[63] Article 9(2) GDPR.
[64] Article 6(1)(b) GDPR.
[65] Article 20(4) GDPR.

a digital marketing company feels it cannot transmit personal data it has collected to another company based on this issue, then it needs to document its reasoning.

Right to object

When data is processed on the grounds of a legitimate interest,[66] data subjects have the right to "object" to the processing of their personal data[67] if the data is used for data marketing purposes or profiling or is processed for research or statistical purposes.[68] Meaning, the right to object under Article 21(2) goes beyond not only serving an advertisement to an individual but also the prohibition of further profiling for the purposes of direct marketing.

When processing relies on the legal basis of legitimate interest, digital marketing companies should use their privacy notice to inform data subjects that they have a right to object at the point of data collection or as soon as possible thereafter. This right should be a separate provision in the data protection notice. Companies should ideally provide a means for requests to be made electronically, preferably in an automated manner of objecting, *i.e.,* an opt-out link. If digital marketing companies are data processors, it should consider allowing data controllers the ability to manage different opt-out lists per data processing purpose.

Organisations should consider the following points when drafting a policy around a data subject right to object:

1. What happens when the data subject asks to "object?"
2. What data does an organisation collect after the right to object?

If a controller has contractually disclosed personal data to a third party, and the data subject has objected to the processing of that data, then the controller must notify those third parties of all changes. If the controller can prove that this obligation is impossible or would require a disproportionate effort, then there is an exception for the controller under Article 19.

The obligation to notify relevant third parties

Where a data controller has disclosed personal data to third parties, and the data subject subsequently exercises any of the rights of rectification, erasure or restriction, GDPR requires the data controller to inform all such third parties that the data subject has exercised those rights, unless doing so is "impossible or involves disproportionate effort."[69] Upon the data subject's request, the controller must also inform the data subject about the identities of any third parties to whom his or her personal data have been disclosed. For organisations that routinely disclose personal data to a large number of third parties, this may become particularly burdensome.

[66] Article 6(1)(f) GDPR.
[67] Article 21 GDPR.
[68] The right to object allows a data subject to object to processing of data on the legal basis of legitimate interest. The revocation of consent allows a data subject to object to processing on the legal basis of consent.
[69] Article 19 GDPR.

Five steps to take now:

1. **Determine whether you are a controller or processor;**
2. **Ensure you have appropriate procedures and policies in place to respond to the data subject rights, including when do you have to respond to data subject rights (Consent versus Legitimate Interest) and how will you respond;**
3. **Having a verification process in place to ensure the data subject has a right to the personal data.**
4. **Make sure your employees in marketing, legal and privacy are properly trained to respond to data subject requests; and**
5. **Update your data protection notices to reflect the data subject rights.**

About the IAB Europe GDPR Implementation Working Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector.

The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

For more information please contact:

Matthias Matthiesen (matthiesen@iabeurope.eu)
Director – Privacy & Public Policy
IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Public Policy Officer
IAB Europe