American Bar Association

What's In Store

What's In Store

Newsletter of the Section of Antitrust Law's Consumer Protection Committee,
Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee

Volume 27, No. 1, April 2018

Editors

Svetlana S. Gans
Federal Trade Commission
sgans@ftc.gov

Patricia A. Conners
Office of the Attorney General of Florida
Trish.Conners@myfloridalegal.com

Ilunga L. Kalala
Kelley Drye & Warren LLP
ikalala@kelleydrye.com

What's In Store is published periodically by the American Bar Association Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee.

The views expressed in *What's In Store* are the authors' only and not necessarily those of the American Bar Association Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee. If you wish to comment on the contents of *What's In Store*, please write to:

The American Bar Association
Section of Antitrust Law
321 North Clark Street
Chicago, IL 60654.

From the Editors

Welcome to the first edition of What's In Store in 2018. Hot off the presses and just in time for spring, this edition features timely interviews with lead enforcers, and much anticipated articles from practitioners and thought leaders at the cutting edge of consumer protection law.

In our first interview, Tom Pahl, Acting Director of the FTC Bureau of Consumer Protection, offers insights into the FTC's top consumer protection priorities in 2018 and explores what the new slate of Commission nominees could mean for the consumer protection mandate of the agency. Next, we interview Herbert H. Slatery III, Tennessee Attorney General, as he approaches the midpoint of his eight-year term. Attorney General Slatery reflects on his office's recent consumer protection accomplishments and discusses the challenges of consumer protection in the near future.

Abigail Stempson, the Director of National Association of Attorneys General's new Center for Consumer Protection, provides us with an overview of the CCP mission and activities, and highlights three co-hosted annual educational conferences as well as the forthcoming launch of a consumer-focused website. We then turn to confidentiality at the NAD as NAD staff attorneys Hal Hodes and Anuradha Gokhale provide clarity on the NAD's treatment of confidential evidence and offer best practices for advertisers and challengers who wish to designate evidence as confidential.

On the privacy and data security front, Alysa Hutnik and Katie Townley offer insights into what we can expect in 2018 as high-profile data breaches and evolving cyber risks move legislators to action. They bring us up to speed on the past year of data breach legislation with a view towards 2018. We round out this edition with some easy conversation around the EU General Data Protection Regulation with Julia Morpurgo. Ms. Morpurgo provides us with an overview of GDPR concepts that are foreign to U.S. practitioners in a must-read (and timely) article.

We hope to see you in on April 11 in Washington, D.C. for the 66th Annual Spring Meeting of the ABA Section of Antitrust Law, the premier event of the year for consumer protection and competition practitioners worldwide. Be sure to join us as we kick off Spring Meeting at 5:30 p.m. on Tuesday, April 10th with Cocktails for Consumer Protection, an informal gathering of your favorite consumer protection colleagues. Inside this edition, you'll find details on all the Spring Meeting consumer protection events and, quite naturally, what's in store for this coming spring.

As always, we welcome your feedback, and we encourage you to contact any of the editors to get involved.

IN THIS ISSUE

Easy Conversation about the Most Complicated Areas of the GDPR

By Julia Morpurgo, CIPP/E

Julia Morpurgo is Associate Counsel at Taboola, Inc. and a Certified Information Privacy Professional in EU privacy law (CIPP/E). This article is intended to provide an overview of the GDPR and is not a definitive statement of the law.

For attorneys in the privacy space, Europe's upcoming General Data Protection Regulation (the "GDPR") has been an all-encompassing whirlwind, where complex concepts have become quick acronyms and daily shorthand. But for the many attorneys who do not advise clients on privacy issues, there are key elements of the GDPR to be familiar with in the upcoming months.

What's the hullabaloo about the GDPR and why should U.S. practitioners care?

The GDPR (officially, EU Regulation 2016/679)[1] is a new privacy regulation that goes into effect on May 25, 2018. Its primary goal is to give individuals within the European Union (the "EU") better control over their personal data and the ways that organizations can use it ("data processing").[2] The GDPR significantly increases requirements for organizations that solicit and retain the personal data of EU residents. This applies to entities both with and without a physical presence in the EU.[3] Non-compliance may result in substantial financial penalties — up to the greater of €20 million or 4% of worldwide annual revenue — so to prepare for compliance, global organizations have been forced to closely examine their processing activities and security parameters with respect to personal data.[4]

So, what is personal data?

The GDPR broadly defines personal data as any information that can be used to identify a natural person (a "data subject").[5] This includes a data subject's name, email, or physical address, and extends to technical information such as IP address, cookies, or device identifiers that can be linked back to the data subject or her device.[6]

---

[1] *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1. The GDPR was adopted on April 27, 2016, but becomes effective on May 25, 2018 after a two-year transition period. The GDPR replaces the existing 1995 Data Protection Directive (Directive 95/46/EC).

[2] Under the GDPR, the definition of "processing" includes any operation, automated or manual, performed with personal data. This may include collecting, recording, organizing, storing, changing, enriching, analyzing, retrieving, consulting, using, disclosing, or transferring personal data. *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 4(2).

[3] *Id.*, Article 3(2). Any organization that collects personal data or behavioral information from someone in an EU country will be subject to the requirements of the GDPR. *See* Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business*, FORBES (Dec. 4, 2017), *available at* https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/#651008876ff2.

[4] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 83(5). *See also* Brian Eaton, *GDPR: Why U.S. Companies Should Care*, PRIVACY & DATA SECURITY INSIGHT (Aug. 16, 2017), *available at* https://www.privacyanddatasecurityinsight.com/2017/08/gdpr-why-u-s-companies-should-care.

[5] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 4(1).

[6] For a detailed discussion, see Phil Lee, *Getting to Know the GDPR, Part 1 - You May Be Processing More Personal Information Than You Think*, FIELDFISHER PRIVACY, SECURITY AND INFORMATION LAW BLOG (Oct. 12, 2015) *available at*

What does the GDPR require?

Organizations that fall within the purview of the GDPR will need to comply with its many requirements:[7]

1. Design data protection safeguards into new products and services from the earliest stages of development
2. Conduct impact assessments of activities that could pose high risks to data subjects' rights
3. Implement adequate security measures and prepare to notify supervisory authorities within 72 hours of a data breach
4. If transferring personal data outside the EU, ensure that receiving entities have adequate safeguards, per EU standards
5. Pre-specify the purpose for processing for each type of data and document the legal basis for such processing activities[8]
6. Maintain thorough records of all processing activities[9]
7. Identify and disclose decisions about data subjects that are made without any human involvement[10]
8. Inform data subjects of the rights they maintain over their data and honor any related requests[11]

Of these requirements, some of the most complex (and unfamiliar to U.S. practitioners) include the requirement for a legal basis for processing, the limits imposed on automated decision-making, and the mandate to honor data subjects' rights, including the right to be forgotten. These are outlined in more detail below.

What is a legal basis for processing?

The GDPR requires that, before organizations begin to process personal data, they identify and publically document a legal basis that supports each specific processing activity. In the broadest sense, processing means using a data subject's personal data in some way. The GDPR outlines six means for lawful processing and an organization should select the most appropriate basis depending on its purpose for

---

http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think. The GDPR definition is broader than U.S. privacy law definitions, which do not include email address or IP address. *See* Rita Heimes, *Explaining the GDPR to an American*, IAPP.ORG (Jan. 30, 2018), *available at* https://iapp.org/news/a/explaining-the-gdpr-to-an-american.

[7] The UK Information Commissioner's Office published a helpful overview of the steps that organizations need to take to prepare for the GDPR. *See* ICO.ORG.UK, *Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now* (May 25, 2017), *available at* https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

[8] No longer may organizations compile personal data in anticipation that it may potentially be of use or value in the future. *See* discussion *infra*, "What is a legal basis for processing?".

[9] At any given time, an organization must have the ability to account for all its processing activities, including, but not limited to: all personal data held about any individual data subject; the entities that the data has been shared with; the purpose for that data's use; and whether that data is subject to automated decision-making. Organizations must also maintain records of all vendors and partners that they share data with and ensure that these partners have adequate safeguards to comply with the GDPR's strict security parameters.

[10] Organizations should pay particular attention to automated decisions that impact a data subject's legal rights. *See* discussion *infra*, "What is automated decision-making and how is it limited?".

[11] Upon a data subject's request, with few exceptions, the organization must honor the data subject's right to access the data free of charge; correct the data; limit or object to the use of the data; or request the data be deleted or shared with another organization. *See* discussion *infra*, "What are data subject access rights?".

processing and its relationship with the data subject.[12]

Organizations may process personal data if necessary to:

1. Fulfill a contractual obligation
2. Comply with a common law or statutory obligation
3. Perform a task in the public interest or
4. Protect someone's life

Organizations may also process personal data if:

5. The individual provides unambiguous consent to do so for a specific purpose[13] or
6. The processing is in the legitimate interest of the organization

What is a legitimate interest?

Legitimate interest is a flexible legal basis that allows organizations to process personal data without having a data subject subscribe or consent.[14] An organization may rely on legitimate interest to process data for regular business operations, such as sending its customers email marketing about a new product, or monitoring authorized user logins to prevent cyberattacks.

However, while flexible, the legitimate interest of the organization is not a "catch all" for activities that do not fall under the other legal grounds.[15] Relying on legitimate interests is permissible if doing so does not infringe on the fundamental rights of the data subject. Personal data must be processed in ways that a data subject would reasonably expect, with a minimal privacy impact on the data subject.

To assess whether a legitimate interest is appropriate, the organization must weigh its business interest against the data subject's fundamental rights, as documented by a comprehensive Legitimate Interest Assessment ("LIA"). The LIA identifies the organization's purpose for processing the personal data (and whether a less privacy-invasive method is available), and why processing it is necessary. Then, the LIA weighs the purpose and necessity against the nature of the data,[16] the potential impacts on the data subject,[17] and whether the organization has implemented appropriate safeguards to protect the data.

---

[12] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 6(1). *See also, Guide to General Data Protection Regulation (GDPR): Lawful Basis for Processing*, ICO.ORG.UK, *available at* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing.

[13] For a discussion of the nuances of unambiguous consent and the circumstances for the more restrictive "explicit consent," see Phil Lee, *The Ambiguity of Unambiguous Consent Under the GDPR*, FieldFisher Privacy, Security and Information Law Blog (June 7, 2016), *available at* http://privacylawblog.fieldfisher.com/2016/the-ambiguity-of-unambiguous-consent-under-the-gdpr.

[14] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 6(1)(f).

[15] Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, ARTICLE 29 DATA PROTECTION WORKING PARTY (Apr. 9, 2014), *available at* http://www.dataprotection.ro/servlet/ViewDocument?id=1086. *See also* Dr. Johnny Ryan, *Why the GDPR 'Legitimate Interest' Provision Will Not Save You*, PAGEFAIR (Mar. 13, 2017), *available at* https://pagefair.com/blog/2017/gdpr-legitimate-interest.

[16] If the processed data is related to children or biometric data, the GDPR requires additional protections that will likely outweigh an organization's legitimate interest.

[17] An assessment of potential impacts should discuss (i) the status of the organization and the status of the data subject (whether the company is in a dominant market position), (ii) the ways data will be processed and whether the company will use profiling, data mining, or other methods considered to be high risk under the GDPR, and (iii) the potential risks of processing or not processing.

Generally, legitimate interest is an effective basis for low-risk processing activities, such as for fraud detection systems, website analytics and diagnostics, or direct marketing purposes.[18] But the legitimate interest rationale may not be relied upon to process sensitive personal data in a way that a data subject would not reasonably expect based on her existing relationship with the organization.[19]

What is automated decision-making and how is it regulated?

Many organizations use tools that automatically evaluate personal data without any human involvement. Such methods can increase business efficiencies and tailor services and products to a data subject's particular needs. However, at their most extreme, these methods can result in exclusionary or discriminatory harm to a data subject.[20]

To protect from such harms, the GDPR outlines restrictions on an organization's decisions that are based solely on automated methods,[21] including profiling (the automated processing of personal data to evaluate characteristics, behaviors, or preferences of a data subject).[22] Because this processing lacks human involvement, the GDPR's restrictions apply if the automated decisions can legally or significantly affect the data subject — for example, an automated decision about whether a data subject should be issued credit or recruited for employment.[23] These requirements uphold the data subject's right to not be subjected to purely automated decisions.[24]

Automated processing may only be used in instances where it is (1) necessary to enter or perform a contract; (2) authorized by law; or (3) based on the data subject's explicit consent. Should an organization use automated decision-making under one of these conditions, it must provide information to the data subject about the processing, offer the data subject simple ways to challenge a decision or request human intervention

---

[18] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Recital 47. *See also* Ben Davis, *GDPR for Marketers: Five Examples of 'Legitimate Interests'*, ECONSULTANCY (Aug. 9, 2017), *available at* https://www.econsultancy.com/blog/69303-gdpr-for-marketers-five-examples-of-legitimate-interests.

[19] *Guide to General Data Protection Regulation (GDPR): Lawful Basis for Processing*, *supra* note 12.

[20] *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, ARTICLE 29 DATA PROTECTION WORKING PARTY (Feb, 6, 2018), *available at* https://iapp.org/media/pdf/resource_center/W29-auto-decision_profiling_02-2018.pdf. *See also* Nicola Fulford & Krysia Oastler, *A Guide to GDPR Profiling and Automated Decision-Making*, KEMPLITTLE.COM (Nov. 17, 2017), *available at* http://www.kemplittle.com/site/articles/kl_bytes/a-guide-to-gdpr-profiling-and-automated-decisionmaking.

[21] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 22.

[22] *Id.*, Article 4(4). Profiling may be as simple as assessing or classifying individuals based on characteristics such as their age, sex, and height, regardless of any predictive purpose. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, *supra* note 20. For a detailed comparison of profiling and automated decisions, see Phil Lee, *Let's Sort Out this Profiling and Consent Debate Once and for All*, FIELDFISHER PRIVACY, SECURITY AND INFORMATION LAW BLOG (July 4, 2017), *available at* http://privacylawblog.fieldfisher.com/2017/let-s-sort-out-this-profiling-and-consent-debate-once-and-for-all.

[23] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Recital 71.

[24] *Id.*, Article 22(1).

instead, and regularly monitor that its systems are working as intended.[25]

What are data subject access rights?

Under the GDPR, personal data does not belong to the organization that collects or processes it; personal data belongs to the individual it identifies.[26] While organizations may use this data to serve customers and fulfill business needs, a data subject may request to exercise her rights to the information at any time.[27] If so requested, the organization must respond to the data subject without undue delay and generally without charge.[28] These rights include:

1. To be informed (typically through a privacy policy)
2. To have access (to know what personal data is held, to know the purpose and legal basis for its processing, and to receive a copy and specific records about this data)[29]
3. To correct inaccurate or incomplete records
4. To restrict processing (the organization may continue to store the data, but may no longer use it)
5. To object (to direct marketing or to the processing of data in the public interest, for research and statistics, or based on legitimate interests);
6. To data portability (the data subject may copy or transfer her personal data to a different service provider) and
7. To erasure (also known as "the right to be forgotten")

Organizations should ensure that their information management systems are well-designed and maintained, so that they can efficiently locate and produce the information requested by any data subjects whose personal data they process.[30]

What is the right to be forgotten?

The right to be forgotten enables a data subject to withdraw her consent or to request that her personal data be deleted if there is no compelling reason for

---

[25] *See Guide to General Data Protection Regulation (GDPR): Rights Related to Automated Decision Making Including Profiling*, ICO.ORG.UK, *available at* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling. *See also* Fulford & Oastler, *supra* note 20.

[26] Heimes, *supra* note 6.

[27] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 12.

[28] Typically, undue delay requires that the organization respond within one month, with limited opportunity to extend an additional two months. *Id.*, Article 12(3). An organization may charge a reasonable fee to cover administrative costs that are necessary to honor a data subject's request, should the request be manifestly unfounded or excessive (typically if repetitive in nature). *Id.*, Article 12(5)(a).

[29] Upon receipt of a right of access request, the organization must provide: (1) whether it processes this data subject's personal data; (2) the purposes of the processing; (3) the categories of data being processed; (4) the categories of recipients with whom data may be shared, particularly if outside the EU; (5) the retention period of the personal data; (6) the data subject's rights to rectify of erase personal data and to restrict or object to the processing; (7) the right to bring a complaint to a supervisory authority; (8) the source of the data, if not collected directly from the data subject; (9) whether any automated processing, including profiling, is applied to the data; and (10) a copy of the personal data being processed. *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 15.

[30] *See Subject Access Code of Practice: Dealing with Requests from Individuals for Personal Information*, ICO.ORG.UK, at 28, *available at* https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf.

the organization to continue to process it.[31] If requested, the organization must erase the data from its systems, unless it has a legal right (freedom of expression), legal requirement (recordkeeping), or legal defense (to support potential legal claims).[32] Organizations should also review whether they need to retain data for the original collection purpose, such as financial records, fraud prevention, or security services.

An organization should provide a publicly available, regularly monitored portal or email address for data subjects to submit a subject access request. The organization may also request additional information that it reasonably needs from the data subject to locate the personal data it holds and to confirm the identity of the data subject (to avoid disclosing to an individual other than the bona fide data subject, which, in turn, could constitute a data breach under the GDPR).[33]

However, some organizations maintain personal data in records that may be impossible to extract or delete, or that may be impossible to connect to the data subject's request.[34] If truly unable to honor the data subject's erasure request,[35] the organization must maintain clear documentation of its reasoning for denying the right, understanding that data protection authorities may narrowly interpret when it is truly appropriate to refuse to honor a request.[36]

Going Forward

As the GDPR's effective date quickly approaches, compliance will continue to be an ongoing process. As enforcement commences and new guidance is issued, legal practitioners — even those that do not work directly in privacy — should stay informed about the European overhaul and think strategically about how the GDPR applies to their clients' data privacy governance and business needs.

Like what you see in this edition?

Want to get more involved?

Please contact Ilunga Kalala at ikalala@kelleydrye.com

---

[31] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Recital 65. Instances of no compelling reason for processing include: (1) the organization does not need the data anymore; (2) the data subject withdraws the consent to processing that she previously provided (and the organization does not need to keep it to comply with a legal requirement); (3) the data subject uses her right to object to the processing; (4) the organization is processing the data unlawfully; (5) a legal requirement for the data to be erased; or (6) the data subject was a child at the time of collection. *Id.*, Article 17.

[32] *Id.*, Article 17(3). Data subjects do not have an unconditional right to be forgotten. If there are other legitimate, legal reasons for the organization to retain and process data, subjects are not entitled to be forgotten. *See* Alex Hanway, *A Deeper Dive into GDPR: Right to be Forgotten?*, GEMALTO SECURITY BLOG (Aug. 16, 2017), *available at*, https://blog.gemalto.com/security/2017/08/16/deeper-dive-into-gdpr-right-to-be-forgotten.

[33] *See Subject Access Code of Practice: Dealing with Requests from Individuals for Personal Information*, *supra* note 30 at 28.

[34] For example, a company may only maintain "pseudonymized data" (where the identity of the data subject has been substituted so that additional information is required to re-identify her). *See generally* Carl Gottlieb, *Right to Erasure*, THE GDPR GUY (Feb. 16, 2017), *available at* https://thegdprguy.com/right-to-erasure.

[35] *EU General Data Protection Regulation (GDPR)*, *supra* note 1, Article 11.

[36] *See Subject Access Code of Practice: Dealing with Requests from Individuals for Personal Information*, *supra* note 30 at 28.