

# Decoding GDPR



VOLUME 102 NUMBER 1 SPRING 2018

## JUDICATURE

Published by the Bolch Judicial Institute at Duke Law. Reprinted with permission. © 2018 Duke University School of Law. All rights reserved. [judicialstudies.duke.edu/judicature](http://judicialstudies.duke.edu/judicature)



## Familiar terms could cause major confusion when GDPR takes effect

**ON MAY 25, 2018, THE GENERAL DATA PROTECTION REGULATION (GDPR) TAKES EFFECT, REPLACING THE AGED EUROPEAN DATA PROTECTION DIRECTIVE CREATED IN THE YEAR 1995.** GDPR intends to harmonize data-protection laws of European Union (EU) member states and strengthen data-protection rights for all individuals within the EU. Unlike the Directive of 1995, GDPR is a regulation rather than a directive, so it does not need to be transposed<sup>1</sup> to EU member states' national laws.<sup>2</sup> Thus, it is directly enforceable.

GDPR also makes data privacy a more critical concern for e-discovery and information governance professionals outside the EU because GDPR has extraterritorial application. Data owners, data handlers, and data processors in the U.S. all have a lot at stake in the changing international business landscape, and the responsibilities of

these groups are only increasing. With globalization, accelerated advancements in technology, data breaches in the news daily and ransomware attacks an ever-growing threat, it's no wonder that the EU has taken action.<sup>3</sup>

While implementation of GDPR-compliant policies and procedures may be costly, the costs of noncompliance could be even higher. Data-protection authorities have a range of corrective powers to enforce GDPR; the most punishing power is the ability of an EU member state's data-protection supervisory authority to levy fines, which could range up to €20 million (\$24.6 million) or 4 percent of a violator's worldwide annual gross revenue for the prior financial year, whichever is higher. This is the nuclear option for the most serious of violations, i.e., not having sufficient customer consent to process data, violations of data subjects' rights, or improper transfer of personal data to

a recipient in a country outside of the EU.<sup>4</sup> Other penalties may be less severe, but still significant. This marks a notable departure from the existing EU privacy regime.

Data protection may feel like a 21st-century issue because the volume of data created every day has dramatically changed the way we collect, store, process, aggregate, link, analyze, and think about information. Fortunately, regulators have been paying close attention to this issue since the mid-1970s. In fact, in 1980 the Organization for Economic Co-operation and Development (OECD) first published its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. This set of recommendations, endorsed by many European nations and the United States, provided the "basic principles" for protecting personal data and set the stage for regulations to come. Notwithstanding this initial common

**This article is the first EDMR GDPR Project publication and was prepared by the following team members in consultation with other project members:**

**ELLE PYLE (CO-LEAD)**, DISCOVERY AND DATA PRIVACY COUNSEL, CIPP/U, CIPP/E, CIPT, CIPM, RUYAKCHERIAN LLP

**LAIA BERTRAN MANYÉ (CO-LEAD)**, ATTORNEY (SPAIN, NY-ADMISSION PENDING); PRIVACY FELLOW, CIPP/US, CIPP/E, DUKE CENTER ON LAW & TECHNOLOGY

**JONATHAN SWERDLOFF**, CONSULTANT, DATA SYSTEMS SPECIALIST, DRIVEN INC.

**LINDA G. SHARP**, ASSOCIATE GENERAL COUNSEL, ZL TECHNOLOGIES, INC.

**REED E. IRVIN**, EXECUTIVE VICE PRESIDENT STRATEGY & MARKETING, VIEWPOINTE

**JIM KOZIOL**, DIRECTOR, TECHNOLOGY AND BUSINESS TRANSFORMATION SERVICES, BDO

**SID JIWNANI**, SOLICITOR, DIRECTOR – EUROPE, KNOVOS

**SAM HOLT**, SENIOR INTERNATIONAL ENGINEER/PRESALES, ACCESSDATA

**VERNA GOODLOE**, SENIOR MANAGER, RECORDS MANAGEMENT, HYUNDAI CAPITAL



LEARN MORE ABOUT EDMR AND THE GDPR PROJECT AT [EDRM.NET](http://EDRM.NET)

baseline, data-protection regulation has evolved in different ways in the EU and the U.S. For example, the EU explicitly recognizes a fundamental right to the protection of personal data in Article 8 of the Charter of Fundamental Rights of the EU,<sup>5</sup> while the U.S. has no such formal recognition.

Many U.S. and EU organizations have begun preparing for GDPR in advance of May 25. Due to GDPR's potential for widespread impact on business, there are many sources of information on how to comply. A very useful 12-step plan for business was created by the United Kingdom's Information Commissioners Office (ICO) (*find the plan at <https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf>*). Despite such resources, organizations and practitioners responsible for compliance are still struggling with the nuances and linguistic confusion between GDPR and U.S. litigation concepts.

To help address these gaps in understanding, EDM — an international professional e-discovery organization now housed at Duke Law School — has assembled a project team of nearly 30 U.S. and EU professionals from the legal and technology sectors to develop “best practices” guidance for conducting data transfers between the EU and the U.S. The goal is to create a reliable and authoritative tool for U.S. organizations, especially e-discovery practitioners. This paper is an initial source that clarifies many of the more important terms commonly used in GDPR and in U.S. e-discovery and privacy contexts that may be confusing, misunderstood, or overlapping.

## BACKGROUND

In 1995, European Union leaders passed the Data Protection Directive 95/46/EC in response to what they saw as an increase in the division of privacy regu-

lations across the EU. This directive was an attempt to align data-protection laws inside the EU and included a provision for transfer of personal data to countries outside the EU. It required that countries outside the EU provide levels of protection for the data comparable to protections within.

Now, 23 years later, advances in technology and increasing sophistication by those attempting to hack or steal data call for stronger protections. Businesses operate in a global context, with personal data moving across borders at a dizzying rate. That is where the EU's GDPR comes in.

GDPR gives EU citizens significant new rights over how their personal data is collected, processed, and transferred by data controllers and processors.<sup>6</sup> For this reason, organizations will need to implement very specific data-protection safeguards or risk potentially astronomical fines for violations. GDPR is designed to harmonize, or standardize, how personal data is treated throughout the EU. The new regulation does give individual member states the flexibility to provide further guidance and refinement, but it serves as a unified baseline on which they may build.<sup>7</sup>

A great debate has arisen over the territorial application of GDPR. Put simply, GDPR applies in two main situations: First, when the processing of personal data takes place within the activities of a controller or processor that is established in the EU, even if the processing itself does not take place on EU territory. This covers the typical situation in which a company outsources its storage or analysis of personal data to a business outside the EU.

Second, GDPR applies to controllers or processors that are not established in the EU, but only if their processing activities relate to two situations: (i) to offer goods or services to data subjects in

the EU; or (ii) to monitor the behavior of the data subjects in the EU (as long as this behavior takes place within the EU).

The ICO puts it most succinctly: “The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.”<sup>8</sup> The bottom line: the GDPR may potentially apply to any data belonging to or handled by a data subject, processor, or controller with an EU situs — and, thanks to the internet, incidental and unwitting contacts with EU citizens likely will widen the risk of unforeseen penalties.<sup>9</sup>

GDPR is a dense regulation consisting of 99 articles and 173 recitals full of general and ambiguous provisions. As with most legislation, an effort to clarify a legal right can lead to confusion. It is critical for organizations to thoroughly understand the terms and details, because the regulation strengthens consent requirements, mandates breach notification, and requires that consumers have access to their personal data, and because noncompliance can lead to harsh financial penalties. U.S.-based organizations must take particular care to understand the similarities and differences among terms used in GDPR and U.S. data regulations and e-discovery contexts, because words and phrases that may seem facially similar have far different meanings under GDPR.

## PERSONAL DATA COMPARED WITH PERSONALLY IDENTIFIABLE INFORMATION

The EU concept of “Personal Data” refers to any information relating to an identified or “Identifiable Natural Person” (“Data Subject”) under GDPR. An Identifiable Natural Person is a person who may be identified, directly or indirectly, by reference to an identifier such as a name, an identification

# ALL PII IS PERSONAL DATA, BUT NOT ALL PERSONAL DATA IS PII.

number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.<sup>10</sup> Personal Data can include IP addresses, email addresses (including work email addresses), and biometric, genetic, and location data.

Conversely, “Personally Identifiable Information,” or “PII,” is a term more commonly used in the U.S. The term PII originated in the U.S. in the National Institute for Science and Technology (“NIST”) working paper Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) SP 800-122. PII includes “any information about an individual maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual’s identity; such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”

Note, however, that the NIST definition is just a starting point. There is no universal definition of PII in the U.S.; several legal rules can apply and color its meaning.<sup>11</sup> For example, each of the following laws relates to different types of PII: HIPAA/HITECH (health PII), GLBA (financial PII), Privacy Act (PII held by U.S. federal agencies), COPPA (Children’s PII), FERPA (students’ PII), FCRA (consumer PII). In addition, each state has its own particular PII definitions contained in breach notification laws.

*The key point is that the definition of Personal Data is considerably broader than the meaning of Personally Identifiable Information.* Personal Data includes any information that can be used to identify

an individual, whether alone *or in combination* with another piece of data. All PII is Personal Data, but not all Personal Data is PII.

## SPECIAL CATEGORIES OF PERSONAL DATA COMPARED WITH PERSONALLY IDENTIFIABLE INFORMATION

Article 9.1 GDPR identifies various categories of sensitive Personal Data as “Special Categories,” which are subject to additional protections. These include: (i) genetic data; (ii) biometric data; (iii) data concerning health; (iv) data concerning a natural person’s sex life or sexual orientation; (v) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.<sup>12</sup>

E-discovery practitioners in the U.S. may recognize some of these categories of data and incorrectly treat them in the same way they would treat PII of a similar type. This mistake may lead to serious consequences. For example, medical records and health data receive additional protection over other types of PII under the U.S. HIPAA protection schema. This does not mean that the PII covered by HIPAA is the same as the Personal Data covered by GDPR, nor does it mean that the standard e-discovery treatment of Medical PII is sufficient for compliance with the EU regulation. Litigation-based requests for document production under the procedural laws of one country (such as the U.S.) can easily run afoul of the data-protection requirements of another, particularly in the case of the EU member states, where GDPR will be automatically incorporated into member states’ national law as of May 25, 2018, even in the absence of any similar provisions in that national law.<sup>13</sup> For *all* data related to EU

data subjects, U.S. practitioners should be careful to ensure compliance with GDPR requirements.

## DATA CONTROLLER COMPARED WITH E-DISCOVERY CUSTODIAN

A “Data Controller” is the natural or legal person(s) who determines the purposes for which, and the manner in which, Personal Data are to be processed. A “Controller” does not necessarily need to be a physical person. It quite often is an organization rather than an individual. In fact, every company that maintains data about an EU citizen is a Data Controller to some extent and is, at a minimum, responsible for processing its employee data or that of its clients. GDPR defines Controller as:

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purpose and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.<sup>14</sup>

In e-discovery, U.S. practitioners typically work with a “Custodian,” who is the “[p]erson having administrative control of a document or electronic file; for example, the data custodian of an email is the owner of the mailbox which contains the message.”<sup>15</sup>

Put in another context, a Custodian can be thought of as a witness or potential witness who is in possession, custody, or control of relevant evidence. Attorneys often interview Custodians of electronically stored information (ESI) in the early stages of a legal matter in order for the attorneys to understand what the Custodian knows about the legal matter ▶

# GDPR PROCESSING INCLUDES, AND LIABILITY ATTACHES TO, A FAR BROADER SPECTRUM OF ACTIVITIES THAN WHAT IS COMMONLY THOUGHT OF IN E-DISCOVERY CIRCLES.

as well as to identify any relevant documents or ESI that are in the Custodian's possession or control. Once the relevant documents are identified, the attorney works with the Custodian to assure that the ESI is preserved for potential use in the litigation.

The GDPR Data Controller does not have a direct U.S. analog. It would be more akin to an e-discovery legal team or records management department than a Custodian, because it is the Controller or the e-discovery team that determines the purpose for which, and the manner in which, any personal data is to be processed.

Thus, the core activity that defines a Custodian is the act of possession or control of potentially relevant ESI, whereas the core activity that defines a GDPR Controller is the power to determine the purpose and the means of processing personal data.<sup>16</sup>

## DATA PROCESSING

The meaning of "Data Processing" is particularly confusing for EU and U.S. practitioners. GDPR defines Data Processing expansively:

Any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination

or otherwise making available, alignment or combination, restriction, erasure or destruction.<sup>17</sup>

In e-discovery, U.S. practitioners commonly refer to data processing as the technical process that is utilized for "[r]educing the volume of ESI and converting it, if necessary, to forms more suitable for review and analysis."<sup>18</sup> Thus, data processing in the U.S. is limited to reducing or massaging the volume of ESI and, in some instances, converting it for easier review. Though this certainly falls within the GDPR definition of processing, the terms are not synonymous. GDPR Data Processing is far broader and can include other activities performed on Personal Data, including those that bear no relationship to e-discovery. GDPR Processing includes any type of handling of Personal Data, or in GDPR language, "any operation performed upon personal data."

Notably, GDPR Processing also includes some forms of *passive* activity or *nonactivity*, which is not reflected in the U.S. concept. For example, under GDPR, *storing* Personal Data is a type of Processing. For those who work in e-discovery, understanding that reviewing documents is also likely to be seen as a form of Processing under the GDPR is crucial. Reviewing documents is "an operation." It certainly could be considered a "consultation" or "use."

The Sedona Conference, in its *International Investigations Principles*,

bases its definition of Processing for all international data transfers on the GDPR definition:

Processing includes any operation, activity, use or application performed upon Protected Data by automatic or other means, such as collection, recording, storage, alteration, retrieval, disclosure or transfer.<sup>19</sup>

Sedona, like GDPR, distinguishes "processing" to include the complete life cycle of Personal Data treatment, from its collection to its destruction. Similarly, it is irrelevant whether the Processing is done by human actors or by technological means. If you are operating in any way on Personal Data, you are Processing it.

Thus, GDPR Processing includes, and liability attaches to, a far broader spectrum of activities than what is commonly thought of in e-discovery circles.

## DATA PROCESSING OF SPECIAL CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION

The EU requires particularly rigorous protection for certain subclasses of personal information. "Special categories of data" are delineated in GDPR Article 9:

... personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biomet-

ric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation . . .<sup>20</sup>

Processing of "special categories of personal data" is strictly prohibited by GDPR, with very few, limited exceptions.

For example, Processing may be permitted with explicit consent of the data subject (the individual who is the subject of the relevant Personal Data) or the performance of specific contracts or processing for specific purposes (vital interest of an individual or public interest).

Data Controllers wishing to process special categories of data must be able to demonstrate that they have a legal basis to do so.<sup>21</sup> GDPR also requires the performance of a Privacy Impact Assessment (PIA) when Processing is likely to result in a high risk to the rights and freedoms of data subjects. Under Article 36, a Data Controller must consult the relevant Supervisory Authority (sometimes also called Data Protection Authority (DPA)) prior to the initiation of Processing if the PIA indicates high risk. Importantly, consent of the data subject will not be sufficient to process special personal data in cases where the risk to individuals' rights are high, unless the relevant Supervisory Authority (or DPA) approves the Processing. This approval is mandatory and U.S. practitioners should take note and get in front of this as early as possible.

The GDPR Article 9 "special categories of data" may seem somewhat analogous to the six "special" categories of data that are afforded additional protection in the United States — health, financial, educational, children's, consumer credit, and PII held by federal agencies. This is, unfortunately, not the case. Though each of these categories of data has its own rules of protection

under U.S. law, those rules do not necessarily parallel GDPR provisions.

For example, a patient's medical data may be processed<sup>22</sup> and even reused in the U.S. upon the patient's consent. Clinical trial research often involves patient data from myriad sources that must be collectively analyzed. Clinical researchers must obtain explicit and informed consent from participating patients to process the data in this manner; once they do that, researchers are free to use the trial data in any manner, including commercially.

Further, unless designated otherwise in the consent itself, if the patient data is scrubbed of identifying information,<sup>23</sup> U.S. patient participants are not required to give consent to the reuse. This is directly contrary to GDPR, which not only requires explicit consent for reuse or sharing of health data, but also allows patients to withdraw their consent at any time.

### GDPR CODE OF CONDUCT

GDPR calls on outside organizations to develop a code of conduct that meets its requirements. Article 40.1 GDPR describes the main goal of a code of conduct as "intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises."<sup>24</sup>

GDPR does not define a code of conduct, but the concept is encapsulated in Article 40, paragraph 2, which states that:

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or Transfer To Third Countries;

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79."<sup>25</sup>

Once an association or body representing a group of entities has completed a draft of the code of conduct, it must submit it for approval to the competent EU Supervisory Authority.<sup>26</sup> The Supervisory Authority will provide an opinion as to whether the code complies with the GDPR, and it shall approve it if it finds that the code provides "appropriate safeguards."<sup>27</sup> If the code of conduct regards processing activities in different member states, the Supervisory Authority will submit the code of conduct to the European Data ►

# FAILURE TO ADHERE TO GUIDELINES AND BEST PRACTICES DOES NOT CARRY SEVERE PENALTIES. VIOLATIONS OF THE GDPR, BY CONTRAST, CAN BRING DISASTROUS CONSEQUENCES.

Protection Board and Commission for opinion and approval.<sup>28</sup>

At all events, the European Board of Data Protection shall create a register with all the approved codes of conduct in order to make them publicly available.<sup>29</sup>

Both GDPR Articles 40 and 41 recognize codes of conduct and encourage entities to use them as a way to meet the security requirements of the GDPR. Indeed, GDPR Article 41.1 allows entities subscribing to a code of conduct to carry out GDPR's mandatory compliance monitoring using their own controllers or processors. Such monitoring is without prejudice to the tasks and powers of competent supervisory authorities pursuant to Article 55 or 56 of GDPR.<sup>30</sup> Thus, GDPR specifically allows, indeed encourages, industries to develop and self-enforce codes of conduct that follow GDPR provisions and ensure GDPR compliance.

Adherence to these codes of conduct serves as a means to demonstrate compliance:

[A]dherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.<sup>31</sup>

## E-DISCOVERY "GUIDELINES"

Many reputable organizations and institutions in the United States have issued useful unofficial e-discovery principles, guidelines, and best practices.

For example, in the preamble to EDRM's *Model Code of Conduct*, EDRM describes "aspirational guidelines intended to serve as a basis for ethical decision-making by all participants in the electronic discovery process."<sup>32</sup>

EDRM has provided multiple examples of such aspirational guidance. The organization has promulgated guidelines for the use of technology assisted review,<sup>33</sup> information governance,<sup>34</sup> as well as the reduction of privacy and security risk.<sup>35</sup> Various courts also have promoted guidelines to suggest best practices in e-discovery.<sup>36</sup> The Sedona Conference, in its *International Principles on Discovery, Disclosure & Data Protection*, provides guidelines built upon its International Litigation Principles to minimize conflict when transferring data to and from the U.S.<sup>37</sup>

This unofficial guidance, however, remains aspirational. There are no enforcement mechanisms in the U.S., nor are these aspirational guidelines legally binding, so this sort of guidance only amounts to suggested best practices. As they are aspirational, such guidance tends to be unmonitored, thus adherence to "guidelines," may not confer any benefit in demonstrating best practices.

This is in stark contrast to GDPR, where adherence to a Code of Conduct, such as described in Articles 40 and 41, serves to demonstrate compliance. It serves not just as an ethical aspiration, but as demonstrable evidence of compliance.

One more critical distinction: Failure to adhere to guidelines and best practices does not carry severe penalties. Violations of GDPR, by contrast, can bring disastrous consequences.

## "CROSS-BORDER" VERSUS "THIRD-COUNTRY" DATA TRANSFER

Another source of potential linguistic confusion is "Cross-Border" data transfer versus "Third-Country Transfer."

Unlike other GDPR terms, which are defined more expansively than their U.S. analogs, the GDPR meaning of "cross-border" data transfers is narrower than the U.S. concept. A U.S. practitioner will understand "cross-border" transfer as any international data transfer, whether into the U.S. or not.

When GDPR references the term "Cross Border," the phrase applies only to the transfer of data within the EU territorial limits of a single controller, processor, or establishment.<sup>38</sup> Transfers that are not within the Union are called "Third-Country Data Transfers" in the GDPR.

GDPR describes "[f]lows of personal data to and from countries outside the Union" as necessary for the expansion of International Trade and Cooperation in

Recital 101 GDPR. Though not specifically defined in GDPR, “third country” means a country outside of the EU, or any country that is not a European Union member state.

Transfer of data to a “third country” means any data transfer made beyond the EU, whether or not the data will be actively used or merely stored in the “third country.” GDPR specifies that data may only be transferred to a “third country” if the European Commission establishes that the “third country” will provide an “adequate” level of protection.

Under the current Directive, the EU Commission has found the level of data protection adequate only in Andorra, Argentina, Israel, Canada (only for data protected by Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA)), Faroe Islands, Guernsey, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. Whether or not these countries will continue to be deemed

adequate under the higher standards that GDPR sets is an open question.

The U.S. level of data protection is, notably, *not* deemed to be “adequate.” U.S. entities certified under the Privacy Shield<sup>39</sup> program, however, have been deemed to provide “adequate” levels of protection. The Privacy Shield has survived its first annual review by the EU Commission. After that review, important recommendations were made to the U.S. government in order for the Privacy Shield to remain valid. It is not known at this time whether the U.S. government will address these issues.

Absent a finding of adequacy, a transfer of data may only occur if certain safeguards are provided. These safeguards include the use of Binding Corporate Rules (BCR), standard contractual clauses as adopted by the European Commission, or the use of an approved code of conduct or certification mechanism. Data may also be transferred in the absence of an adequacy

decision only with the permission of the data-protection authority.<sup>40</sup>

The distinction drawn by GDPR between “cross-border” and “third-country” data transfers is unique. Unofficial data-transfer principles, guidelines, and best practices may not recognize the same distinction.

## CONCLUSION

GDPR is designed to harmonize data-protection laws of EU member states and strengthen data-protection rights for all individuals within the EU. Severe penalties for noncompliance coupled with bright-line rules and a broad scope will undoubtedly ensure that. For U.S. practitioners, one of the first and most important steps in preparing for May 25 should be undertaking a study of GDPR requirements and terms, with particular attention to the terms that may seem *deceptively* familiar.

<sup>1</sup> Transposition is the process by which a EU member state’s legislative branch adopts a national statute or law to implement an EU Directive. This is only necessary when the EU creates directives, which are not directly enforceable by member states. By contrast, EU regulations are directly enforceable even if the text of the regulation is not present in the national law of a member state.

<sup>2</sup> As stated below, GDPR provides some flexibility to member states, which may develop into implementation differences in the different member countries. For example, article 8 GDPR establishes that member states can set their own age limit for when children can give valid consent between 13 and 16 years old.

<sup>3</sup> The European Commission first proposed to modify the EU’s data protection rules in 2012. It took several years for the EU to reach an agreement on the final text. *See The History of the General Data Protection Regulation*, European Data Protection Supervisor, [https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation\\_en](https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en) (last visited Mar.

17, 2018). *See also* Commission Regulation 2016/679, rec. 5–7, 2016 O.J. (L119) 1(EU) [hereinafter GDPR] (explaining the reasons for enacting the GDPR).

<sup>4</sup> GDPR, *supra* note 3, art. 83.5.

<sup>5</sup> Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C326) 2.

<sup>6</sup> See discussion of EU vs. U.S. data processing *infra*.

<sup>7</sup> *See supra* note 2.

<sup>8</sup> *Guide to the General Data Protection Regulation (GDPR)*, Information Commissioner’s Office, <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/> (last visited March 17, 2018).

<sup>9</sup> Note that under Recital 23 of the GDPR the mere accessibility of a controller’s or processor’s website in the EU is insufficient to determine the applicability of the GDPR. However, Recital 23 of the GDPR identifies certain factors that can trigger the applicability of the GDPR, such as the use of language or currency of one or more EU countries on the website.

<sup>10</sup> GDPR, *supra* note 3, art. 4. *See also id.*, rec. 26;

*id.*, rec. 27; *id.*, art. 2.2; *id.*, art. 2.3.

<sup>11</sup> *See* Fed. R. Civ. P. 5.2; Fed. R. Crim. P. 49.1; Fed. R. App. P. 25(a)(5); Fed. R. Bank. P. 9037 (prohibiting references to certain personal data identifiers in public filings, including social security number, tax-payer identification number, birth date, financial-account number, and name of a minor).

<sup>12</sup> GDPR, *supra* note 3, art. 9.1, art. 4 (13), art. 4 (14), art. 4 (15). *See also id.*, rec. 34; *id.*, rec. 35.

<sup>13</sup> *See supra* note 1.

<sup>14</sup> GDPR, *supra* note 3, art. 4 (7).

<sup>15</sup> *Data Custodian*, EDRM, <https://www.edrm.net/glossary/data-custodian/> (last visited Mar. 17, 2018) (citing Fios, EDiscovery Glossary, [http://discoveryresources.org/01\\_electronic\\_discovery\\_glossary.html](http://discoveryresources.org/01_electronic_discovery_glossary.html), Vinson & Elkins LLP Practice Support, EDD Glossary and RSI, Glossary).

<sup>16</sup> By “processing” we mean GDPR “processing,” Further described *infra*.

<sup>17</sup> GDPR, *supra* note 3, art. 4.

<sup>18</sup> *Processing Phase*, EDRM, <https://www.edrm.net/glossary/processing-phase/> (last visited March 17, 2018).

<sup>19</sup> *Sedona International Investigations Principles*, Sedona Conference, <https://thesedonaconference.org/publication/International%20Investigations%20Principles> (last visited March 18, 2018).

<sup>20</sup> GDPR, *supra* note 3, art. 9.1. See also *id.*, rec. 10; *id.*, rec. 34; *id.*, rec. 51.

<sup>21</sup> GDPR, *supra* note 3, art. 9.2.

<sup>22</sup> In both the U.S. and EU concept of Processing.

<sup>23</sup> De-identification is when individual identifiers such as name, social security number, or date of birth are removed.

<sup>24</sup> GDPR, *supra* note 3, art. 40.1.

<sup>25</sup> GDPR, *supra* note 3, art. 40.

<sup>26</sup> GDPR, *supra* note 3, art. 40.5.

<sup>27</sup> GDPR, *supra* note 3, art. 40.5.

<sup>28</sup> GDPR, *supra* note 3, art. 40.7–40.9.

<sup>29</sup> GDPR, *supra* note 3, art. 40.11.

<sup>30</sup> GDPR, *supra* note 3, art. 4(11).

<sup>31</sup> GDPR, *supra* note 3, art. 32.3.

<sup>32</sup> *EDRM Model Code of Conduct*, EDRM, <https://www.edrm.net/frameworks-and-standards/edrm-model-code-of-conduct/> (last visited March 17, 2018).

<sup>33</sup> *Technology Assisted Review*, EDRM, <https://www.edrm.net/frameworks-and-standards/technology-assisted-review/> (last visited March 17, 2018).

<sup>34</sup> *Information Governance Reference Model*, EDRM, <https://www.edrm.net/frameworks-and-standards/information-governance-reference-model/> (last visited March 17, 2018).

<sup>35</sup> *Privacy and Security Risk Reduction Model*, EDRM, <https://www.edrm.net/frameworks-and-standards/privacy-and-security-risk-reduction-model/> (last visited March 17, 2018).

<sup>36</sup> See, e.g., *E-Discovery (ESI) Guidelines*, United States District of Northern California, <http://cand.uscourts.gov/eDiscoveryGuidelines> (last visited March 17, 2018); *E-Discovery Plan Guidelines*, Superior Court of Delaware, [https://courts.delaware.gov/superior/pdf/cld\\_appendix\\_b.pdf](https://courts.delaware.gov/superior/pdf/cld_appendix_b.pdf) (last visited March 17, 2018); *Guidelines for the Discovery of Electronic Documents in Ontario*, [http://www.oba.org/en/pdf\\_newsletter/E-discoveryguidelines.pdf](http://www.oba.org/en/pdf_newsletter/E-discoveryguidelines.pdf) (last visited March 17, 2018).

<sup>37</sup> The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection* (June, 2018), [https://s3.amazonaws.com/IGG/publications/The+Sedona+Conference+Practical+In-House+Approaches+for+Cross-Border+Discovery+and+Data+Protection\\_June++2016+Version.pdf](https://s3.amazonaws.com/IGG/publications/The+Sedona+Conference+Practical+In-House+Approaches+for+Cross-Border+Discovery+and+Data+Protection_June++2016+Version.pdf) (citing The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation*).

<sup>38</sup> GDPR, *supra* note 3, art. 4.

<sup>39</sup> *EU-US Privacy Shield*, European Commission, [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en) (last visited March 17, 2018).

<sup>40</sup> See GDPR, *supra* note 3, art. 49 (certain exceptions apply including the explicit and voluntary consent of the data subject for the transfer, necessity of data transfer for the performance of a contract between the data subject and the controller, or necessity of safeguards).



**Huntington Bank**  
is a proud sponsor  
of Judicature.

 **Huntington**  
huntington.com

Member FDIC.  and Huntington® are federally registered service marks of Huntington Bancshares Incorporated. © 2017 Huntington Bancshares Inc.