dri™
Center for Law and
Public Policy

What Is the GDPR?

If You and Your Clients Are Still Asking That on May 25, 2018, You May Have a Serious Problem.

✓Includes a Preparedness Checklist

DRI
55 West Monroe Street, Suite 2000
Chicago, Illinois 60603
dri.org

Produced in the United States of America
ISBN: 978-1-63408-033-0

What Is the GDPR?

By Laura Clark Fey, Susan Gunter, Judy Krieg, John Magee, Winston Maxwell, and Tobias Schelinski

dri Center for Law and Public Policy™

Table of Contents

The EU General Data Protection Regulation (GDPR) will take effect on May 25, 2018. Penalties for non-compliance can be as high as 20 million euros or 4 percent of annual worldwide turnover. The GDPR has very broad territorial reach—it applies not only to European entities, but also to entities located outside of the European Union that offer goods or services to people in the European Union or that monitor the behavior of people in the European Union. The GDPR will affect businesses, including DRI members and their clients, around the globe. This white paper seeks to provide a basic introduction to the GDPR for DRI attorneys.

Transport yourself to the near future of May 2018, to a small shop in Kansas City, Missouri, USA. The store is happy to receive an order from an EU resident and drop the goods into international parcel delivery. As a matter of course, the store processes the personal data of the EU resident, as it would for a customer anywhere. Processing the personal data for this sale, however, subjects the store to the European Union's General Data Protection Regulation—the GDPR. That regulation's powerful enforcement mechanisms reach to this event—and so many more around the globe—that lack any obvious relation to commerce in the European Union. This white paper of the DRI Center for Law and Public Policy examines the GDPR in a manner that should be understood by any lawyer representing businesses.

Who Should Care About the GDPR?

Almost every entity that conducts any business in Europe or that receives any EU personal data[1] from clients should care about the GDPR. The GDPR has very broad territorial reach. The GDPR's applicability is not limited to organizations located in the European Union or even the European Economic Area; it is not limited to multinational organizations; and it is not limited to technology companies, or for that matter, to any specific type of entity.

To whom and under which conditions will the GDPR apply? First, the GDPR will apply to establishments[2] in one or more EU Member States that process[3] personal data "in the context of the activities" of such entities.[4] The GDPR will apply even if an entity is not processing EU personal data in the European Union. For example, an international law firm with offices in the European Union will need to comply with the GDPR

---

[1] The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, Article 4(1).

[2] An establishment is "the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." *See* GDPR, Recital 22.

[3] The GDPR defines "processing" as "any operation or set of operations which is performed on personal data or on 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." GDPR, Article 4(2).

[4] GDPR, Article 3.

when the human resources department in its US headquarters processes personal data of attorneys and staff located in the European Union.

Second, the GDPR also will apply to the EU personal data processing activities of entities that are not established in the European Union if such processing activities are related to (1) the offering of goods or services to data subjects in the EU, regardless of whether a payment from a data subject is required; or (2) the monitoring of data subjects' behavior within the European Union. For example, the GDPR will apply to a retail store located only in Kansas City when the store processes personal data of EU residents that it receives when EU residents purchase goods offered to EU residents on one of the store's retail websites. As another example, the GDPR will apply to a technology company located in Mumbai that tracks EU residents' internet behavior.

Third, even entities that are not established in the European Union, do not directly offer goods or services to EU residents, and do not monitor the behavior of EU residents will be subject to the GDPR if they collect, store, or otherwise process EU personal data on behalf of their clients. For example, the GDPR will apply when attorneys in a global law firm's Singapore, Toronto, and Cape Town offices review EU personal data in performing legal work for one of the firm's clients. In fact, clients subject to the GDPR are likely to insist that their law firms and other entities to which they transfer EU personal data comply with the GDPR's requirements and enter an agreement to do so.[5]

It also should be noted that the GDPR will apply to entities regardless of whether they have three employees or 300,000 employees. The Irish Data Protection Commissioner Helen Dixon has said,

> The GDPR is big news because it can't be business as usual for any type of company… after May 2018. If it is business as usual after that point, there will be consequences for companies and organizations, whether they are big or small, public or private, and those consequences will be very significant.[6]

Those significant consequences will be addressed in this white paper after a discussion of the GDPR's reach.

---

[5] *See* GDPR, Article 28.

[6] Harry Leech, *New Data Rules Mean It Can't Be 'Business as Usual'—Helen Dixon*, Independent.IE (2 Apr. 2017), http://www.independent.ie/datasec/new-data-rules-mean-it-cant-be-business-as-usual-helen-dixon-35585883.html.

What Is It?

Background

The GDPR is a critical reform for the EU digital, single-market agenda and has been a work in progress since 2012. The predecessor protection regime, the Data Protection Directive,[7] has been applied uniquely in each EU Member State. This resulted in the Data Protection Directive framework being interpreted differently across the European Union. As the GDPR is a regulation, it will be immediately effective in May 2018, without the need for implementing national legislation in EU Member States. The GDPR aims to ensure consistent protection of personal data through a harmonized legal framework. The significant advancements in technology since the Data Protection Directive was drafted also necessitated the legislative overhaul.

Data Protection Principles

Data protection principles are the cornerstone of the GDPR, and they provide the conditions on which personal data may be processed. The data protection principles are broadly similar to those set out in the Data Protection Directive; however, there are new elements to the principles that enhance the protection in relation to the processing of personal data. The key principles as set out in the GDPR include the following:

- **Lawfulness, fairness, and transparency:** Personal data must be processed in a manner that is lawful, fair, and transparent. Organizations are required to provide extensive information to data subjects in relation to the processing of their personal data.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- **Purpose limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.
- **Data minimization:** Personal data gathered must be adequate, relevant, and limited to what is necessary. This principle has changed under the GDPR so that organizations are obliged to ensure that personal data is limited to what is necessary for the purpose for which processing is carried out.
- **Accuracy:** Personal data must be accurate and kept up to date where necessary. Reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.
- **Storage limitation:** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
- **Accountability:** Organizations must be able to demonstrate compliance with the data protection principles. This principle shifts the burden of proof to the controller to be able to demonstrate compliance with the data protection principles and the controller's obligations under the GDPR.

Organizations must incorporate the data protection principles into their business processes and be able to demonstrate compliance with the data protection principles.

Legal Obligations

The implementation of the GDPR brings about a number of sweeping changes to the existing rules, some of which (such as mandatory personal-data breach reporting) are likely to lead to an increase in privacy and cybersecurity litigation.

The data protection principle of accountability places a number of obligations on organizations to ensure compliance with data governance. All organizations must implement measures to show that they have considered and integrated the data protection principles into their data-processing activities. Other obligations include the mandatory conduct of data protection impact assessments, the appointment of data protection officers, and the maintenance of records of processing activities.

Businesses that process data (such as law firms) are not immune to the new rules. Both controllers (*i.e.*, a natural or legal person who, alone or jointly with others, determines the means and purposes of processing) and processors (*i.e.*, a natural or legal person who processes personal data on behalf of the controller) are subject to obligations in relation to the reporting of personal data breaches, and the GDPR specifies that controllers must report a personal data breach to a supervisory authority without undue delay, and where feasible, no later than 72 hours after becoming aware of it.

There are increased obligations under the GDPR with respect to vendor management. Data processing agreements must be in writing, including in electronic form, and they are required to prescribe more detailed terms, such as specifying the subject matter, duration, nature, and purpose of the processing and that data transfers outside the European Union can only take place based on the documented instructions of a controller. Data-processing agreements and data transfer contracts between US organizations and those based in the European Union will require serious consideration in light of the additional obligations under the GDPR.

The enhanced rights of data subjects under the GDPR bring about additional obligations for organizations and are likely to represent significant operational and technical challenges. Organizations will be required to ensure that their policies and procedures are updated to respond to data access requests within the shorter time frames mandated by the GDPR. The GDPR incorporates existing data subject rights, with some revisions, including the right to access, the right to rectify inaccurate or incomplete personal data, the right to object to processing, and the right of the data subject not to be subject to a decision based solely on automated processing that produces significant legal effects or similarly affects the data subject (*i.e.*, rejecting a credit application or job application based entirely on an algorithm with no human intervention). Organizations will also have to implement processes to accommodate the new rights of data subjects, such as the right to the erasure of personal data (although the "right to be forgotten" was recognized by the Court of Justice of European Union, it was not included in the text of the Directive); the right to restrict the processing[8] of personal data; and the right to data portability. Organizations must also make certain that staff are adequately trained to deal with such requests to ensure that any claims, investigations, or litigation arising can be responded to effectively.

The data protection principles of lawfulness, fairness, and transparency also increase the obligations under the GDPR because organizations will need to provide extensive information to data subjects in relation to the processing of their personal data. Organizations will also have to review the grounds for lawful processing relied upon because organizations will be required to provide data subjects with notice of the legal basis or bases for the processing activities. Organizations should be aware that the GDPR makes it much more difficult for organizations to rely upon consent as their lawful basis for processing. The new rules provide that consent must be provided by a statement or clear, affirmative action. Additionally, consent will only be valid if it is freely given, specific, informed, and unambiguous. It must be as easy to withdraw consent as it is to give consent.

[8] Processing is defined in Article 4(1) of the GDPR as any operation or set or operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Why Is It Such a Big Deal?

Onerous Obligations

Organizations must review their data processing activities and determine an approach to compliance with the onerous obligations imposed by the GDPR. In light of the territorial scope of the GDPR, any US- or non-EU-established organizations that target or monitor data subjects in the European Union will also be required to review their data processing activities and implement various changes within the organization to ensure compliance with the GDPR.

All customer-facing documentation, such as privacy statements and client inception forms, will require updating because organizations are required to provide extensive information to data subjects in relation to the processing of personal data in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. To the extent that organizations have customers, clients, or employees in the EU, their data-processing operations will need to be reviewed to determine whether any personal data processed is unnecessary and to update their business processes accordingly.

The data governance obligations require substantial preparation and resources ahead of the implementation of the GDPR. The data protection principles must be incorporated into all data processing activities, and organizations must implement or amend technical and organizational measures in light of these principles. Organizations will also have to implement a compliance program tailored to the specific activities of each organization, incorporating various elements, such as conducting data protection impact assessments, creating and maintaining records of processing activities, appointing a data protection officer where required, and developing a data breach notification procedure. Organizations must also review and map international data flows and consider whether their data transfer mechanisms are appropriate under the GDPR.

The most widely used data transfer mechanisms relied upon by US companies to govern transatlantic data transfers are the EU-US Privacy Shield, standard contractual

clauses, and binding corporate rules. Due to some uncertainty around the status of these mechanisms, many organizations choose to adopt a layered approach that does not exclusively rely upon any one of them. With regard to data transfer agreements, it is likely that contractual negotiations around liability caps and exclusions will become protracted as a result of the increased obligations and significant fines under the GDPR. With the stakes so much higher, disputes and litigation centered on such contracts are likely to become more commonplace. Organizations should be prepared for such protracted contractual negotiations and anticipate disputes and litigation.

Onerous Penalties

The penalties mandated by the GDPR are considered to be the most significant changes under this new data protection regime, and such penalties are reinforced by the enhanced powers of supervisory authorities. Supervisory authorities are the independent, public authorities established by each EU Member State responsible for monitoring compliance with data protection. Supervisory authorities are empowered to issue warnings to organizations that their intended processing operations are likely to infringe upon the GDPR, to issue various orders to organizations to comply with data subjects' requests, and to order the suspension of data flows to a recipient in a third country, such as the United States.

Depending on which provision of the GDPR is breached, supervisory authorities can impose administrative fines up to the higher of €20,000,000 or 4 percent of global annual turnover (*i.e.*, revenue), or up to the higher of €10,000,000 or 2 percent of global annual turnover. The purposes of the fines are to be effective, proportionate, and dissuasive, and the behavior of an organization is taken into account when levying a fine for a breach of the GDPR. Organizations will have to assess their liability exposure carefully in light of such potentially severe administrative fines. In assessing potential risks of non-compliance, organizations should consider not only the GDPR's onerous fines, but also the potential for legal actions by data subjects, significant negative publicity relating to any enforcement actions or data subject actions, and the corresponding adverse effect on public opinion.

Multiple Paths of Enforcement

Under the GDPR there are numerous enforcement paths to potential actions against organizations. Data subjects have the right to lodge a complaint with supervisory authorities where their personal data is processed in a way that does not comply with the GDPR. An action can be brought where a supervisory authority fails to deal properly with a complaint. Data subjects can take action directly against a controller or processor where their rights have been infringed, and proceedings can be brought either in the Member State in which the initiating data subject resides or in any location where the controller or processor has an establishment.

Data subjects can be represented by a not-for-profit body active in the field of data protection. Such bodies can lodge a complaint and pursue an effective judicial remedy

on behalf of data subjects and can also exercise the right to receive compensation. These rights are expected to give rise to a significant increase in the number of compensation claims brought against organizations in a collective manner, similar to class action litigation in the United States.

An infringement of the GDPR can also give rise to a right of compensation from the controller or processor, and any person who has suffered material or *non-material* damage, such as loss of control over his or her personal data, identify theft, financial loss, discrimination, or any other significant economic or social disadvantage to the person concerned, will have the right to receive compensation. In addition to the administrative fines that are potentially applicable under the GDPR, organizations may also be required to compensate individuals, regardless of whether individuals have suffered financial damage or not. Coupled with the ability to bring a type of "class action" claim, as highlighted above, it is expected that the volume of data privacy claims and litigation related to non-financial types of loss (such as distress or reputational damage) will increase.

The various methods of enforcing the obligations of organizations under the GDPR empower data subjects to be vigilant with respect to data protection rights. As data subjects may bring proceedings in their country of habitual residence, multinational organizations could potentially face regulatory investigations and court actions across a number of EU Member States.

Where Does the GDPR Intersect with My Business?

This section outlines the GDPR issues that need to be considered for various types of business models. A fuller explanation of the steps that are needed to address these issues is set out below.

Sales of Goods and Services to EU Residents

For entities that offer goods and services to EU residents, even those entities that have no EU offices or establishment, there are a number of GDPR issues to consider. The first step will be to undertake an information audit, and in some circumstances, a data protection impact assessment (DPIA), of whatever personal data the entity already holds. Entities need to understand the personal data that they hold, where it came from, and with whom it is shared.

Privacy notices and terms and conditions for the collection and use of personal data must be reviewed and updated. Among other requirements, the organization's privacy notice needs to set out the purposes and lawful bases for all processing activities, the data retention period (or the criteria used to determine such period), information concerning data subject rights, and the right to complain to a data protection authority. It is important to consider how the entity collects personal data and how that personal data is used in marketing (such as profiling and behavioral advertising). Any necessary consent needs to be considered. How is consent sought, recorded, and managed? Consent processes will almost certainly need to be updated due to the enhanced GDPR requirements (including requiring positive opt-in).

Documentation systems need to be implemented to demonstrate the entity's compliance with the GDPR. This will include the following:

- records of processing activities;
- data protection by design and default;

- lawful bases for processing;
- data protection impact assessments; and
- data-breach response processes.

New or updated procedures will need to be in place to help ensure the entity's compliance with all individual rights under the GDPR, including but not limited to:

- the right to access (subject access requests);
- the right to erasure (right to be forgotten, data deletion); and
- the right to rectification.

Entities to which the GDPR applies also will need to consider whether a data protection officer must be designated. Even if appointment of a data protection officer is not legally required by the GDPR or Member State law, it is advisable to select one or more persons with primary responsibility for GDPR compliance.

Websites and Applications

In addition to the issues set out above for sales of goods and services, another issue to consider is data portability. The right to portability may not apply to all entities. The right to portability is only triggered when processing is carried out by automated means (*i.e.*, electronic), and the lawful basis for processing is consent or a contract to which the data subject is a party. The scope of the right to data portability is also limited to personal data that the data subject has provided to the controller. However, this has been broadly interpreted to include not only personal data actively and knowingly provided by the data subject, but also to "observed data provided by the data subject by virtue of the use of the [controller's] service or device" (*i.e.*, a person's search history, traffic data, or location data).[9] Although there are some limits to the scope of the right to portability, entities that process personal data that fall within its requirements need to have a process in place to provide the personal data in the appropriate format when requested by an individual.

Websites and applications entities have a particular need to ensure that they are properly handling any personal data relating to children. This includes verifying ages and obtaining parental or guardian consent when consent is the lawful basis for processing.

Data protection by design and default takes on additional importance for website and application companies. When assessing the entity's existing products or developing new products, a technology functionality gap analysis should be conducted. This compares the operational performance of the products against the requirements of the GDPR. Data controllers need to be able to show affirmatively that they are taking appropriate technical and organizational measures to comply with the GDPR. These entities

[9] Article 29 Working Party, Guidelines on the right to data portability, at 10 (5 Apr. 2017).

will need to maintain a repository of documentation, including design plans, functional testing, and assessment documentation.

Third-Party Service Providers

Additional care needs to be taken when selecting any third-party providers that access and process personal data for a company (organization, firm), including cloud service providers, outsourced human resource function providers, and e-discovery vendors. Under the GDPR, data processors may be liable to data subjects for damages resulting from infringements of applicable GDPR obligations or for their failure to follow a controller's lawful instructions. Processors and controllers may be held jointly and severally liable for harm caused by processing activities unless they can prove they did not contribute to the harm. Similarly, there is joint and several liability under the GDPR for joint controllers involved in processing activities if they are in any way responsible for the event giving rise to the damages.

Factors to bear in mind when selecting third-party service providers include the strength of their GDPR compliance and IT security measures. The third-party service provider (similar to the controller) must have in place technical and organizational measures to ensure an appropriate level of security. Controllers must only use processors that provide sufficient guarantees of their abilities to implement these technical and organizational requirements. Controllers and processors must also maintain certain documentation, including records of processing activities.

The location of a third-party service provider is also important, particularly if the third-party service provider is located outside the European Union in a country that has not been deemed by the European Commission to provide adequate personal data protection.

Entities subject to the GDPR also will need to ensure that they have proper contractual terms in place with current and future processors. Contract addenda will need to be prepared for current contracts and new contractual templates prepared for future contracts. The GDPR contracting requirements set forth in Article 28 of the GDPR include these, among others:

- Processors must only process data as instructed by controllers.
- Processors must use appropriate technical and organizational measures to comply with the GDPR.
- Processors must delete or return data to the controller once processing is complete.
- Processors must submit to specific conditions before subcontracting with other processors.

In addition to ensuring that all Article 28 requirements are covered in contracts, entities should confirm that terms are defined properly in accordance with

the GDPR and that desired indemnification, warranty, and termination provisions are incorporated.

Data controllers need to keep records of all data processing that is outsourced to third parties. If an individual invokes certain rights (*i.e.*, right to be forgotten, right to rectification), the data controller must be able to notify the third party of the erasure or rectification to be made.

Mergers & Acquisitions

When putting data into a data room for M&A due diligence purposes, it will invariably include personal data. To the extent possible, the amount of personal data should be kept to a minimum. This could mean redacting personal data shared, pseudonymizing data shared, or limiting employee data shared to only specified employees who are crucial to the deal. The lawful basis for processing the data needs to be considered, as well as the location of the data. Proper notice and, if applicable, consent should be confirmed before any personal data is shared. If the data room is located outside of the European Union, or if the data is accessed by persons (including lawyers) who are located outside of the European Union, a proper legal basis for transferring the data needs to be confirmed. Additionally, in all cases, appropriate technical and organizational security will need to be ensured.

The GDPR can also affect deal value. From a potential buyer's perspective, due diligence will need to encompass the target entity's compliance with the GDPR and any potential liability that may already exist. This might trigger the need for indemnities or warranties. Any new buyer also needs to consider the language in any consent that customers have given in connection with marketing. Specifically, does the language of the consent include any subsequent purchasers of the business and will new consents need to be obtained? Any post-acquisition integration plan should fully consider how the business will maintain GDPR compliance in the future. If the merger or acquisition activity involves an entity that is new to GDPR compliance (*i.e.*, a non-EU entity acquiring an EU entity), this integration plan could be considerable.

Human Resources

Just as entities that sell goods and services to EU residents need to consider how they are collecting, processing, and handling that data, any entity that employs EU residents must to do the same for the personal data of its employees and potential employees. Recruiting processes, pre-employment checks, data retention, and employee policies and procedures (including the Fair Processing Notice) all will need review and updating to ensure compliance with the GDPR (and compliance with the applicable legal obligations set forth by specific Member States). Changes to the Fair Processing Notice might also trigger changes to employment contract documents.

Entities will need to confirm an appropriate legal basis for processing job applicant and employee personal data, particularly because consent is unlikely to be considered

an appropriate basis for processing employee personal data. Consent from employees is unlikely to be considered "freely given" as required because of the imbalance in the employer–employee relationship.[10] Employers will need to consider alternative legal bases for processing, such as the employment contract, EU or Member State legal obligations, and legitimate interests.

Any organization that employs EU residents will need to be prepared to address data subject access requests in a timely manner, as well as other data subject rights requests from employees, which may become even more frequent under the GDPR in light of the fact that organizations will not be permitted to charge even nominal fees for responding to data subject requests, unless requests are manifestly unfounded or excessive. An employee can also submit a "right to be forgotten" request to ensure that personal data is not stored any longer than necessary. Certain human resource processes may fall into the category of profiling (recruitment filters, large-scale redundancy), so care may need to be taken to ensure that decision making is not entirely automated.

Cross-Border Discovery and Disclosure and Internal Investigations

Personal data is often collected and reviewed as part of litigation discovery and disclosure, or for internal investigations. Organizations should seek to limit such collection, review, and production of personal data to the fullest extent possible through actions such as negotiating with opposing counsel and appealing to judges to limit the required production of personal data to the maximum extent possible.

The legal basis for processing such information must be taken into consideration. Even if an internal investigation is warranted, consent might be required to process certain personal data (*e.g.*, where special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, or data concerning health, are involved, explicit consent is the only appropriate basis for processing).

The location of the review is important, particularly if there is a need or desire to transfer certain personal data outside of the European Union. This can occur if EU data is reviewed for purposes of US litigation or reports to US authorities, for example. Ideally, the data should be first reviewed within the European Union to help ensure that only relevant personal data is transferred outside of the European Union. Organizations should also consider measures such as in camera review of personal data and protective orders. Where transfer outside the European Union is necessary, steps should also be taken to help ensure the lawfulness of the transfer, such as through standard contractual clauses or through the organization's participation in the EU–US Privacy Shield.

[10] *See* Article 29 Working Party, Opinion 2/2017 on data processing at work, at 23 (June 2017).

When Do Entities Need to Be Compliant with the GDPR?

The GDPR takes effect on May 25, 2018, so it is highly recommended that entities begin preparing as soon as possible. As noted above, the GDPR is not "business as usual," and business processes do not change overnight. GDPR preparation takes time. It takes time to obtain buy-in from executives before even beginning to focus on GDPR readiness. It takes time to assess compliance gaps, develop a prioritized compliance action plan, and obtain the approval and budget required to implement the compliance action plan effectively. And it takes time to implement wide-ranging GDPR-readiness activities—from identifying EU personal data and data flows and developing a targeted data map, to developing GDPR-compliant privacy policies, procedures, notices, and consent mechanisms, to developing solutions for timely addressing data subject rights-related requests.

Studies have shown that GDPR compliance will require a serious financial commitment, so it is important to act quickly to secure a sufficient budget for GDPR preparation. According to a study conducted by TrustArc, 83 percent of privacy professionals reported that they expect GDPR-related compliance spending for their entities in 2017 and 2018 to be at least $100,000, with 40 percent of respondents planning to spend at least $500,000 to become GDPR compliant.[11] Seventeen percent expected to spend in excess of $1 million. That number increased to 20 percent when only entities with between 1,000–5,000 employees were considered.

[11] *See* TrustArc, *Privacy and the EU GDPR* (2017) ("2017 TrustArc Study"), https://info.trustarc.com/Web-Resource-PrivacyGDPR-ResearchFullReport-Q32017_LP.html. Survey respondents included 204 privacy professionals. TrustArc targeted IT and legal professionals at small (defined as 500–1,000 employees), mid-sized (defined as 1,000–5,000 employees), and large (defined as over 5,000 employees) companies that were subject to the GDPR. Further, 92 percent of the companies surveyed were based in the United States or Canada.

In another survey, 77 percent of survey respondents from entities with over 500 employees were budgeting over $1 million to meet their GDPR compliance obligations. Nine percent of those respondents asserted that they were budgeting over $10 million to meet their obligations.[12]

Obtaining approval for a budget is a critical step, but it is only the beginning of the process of moving from "business as usual" to GDPR compliance. Indeed, the GDPR's expanded legal obligations require organizations to undertake significant efforts to prepare to address their obligations and to prepare for the GDPR's effective date. Many entities have already started preparing for the GDPR. In the TrustArc study, 95 percent of survey respondents asserted that they had begun preparing to meet their obligations under the GDPR.[13] And in an earlier survey of C-suite executives in the United States, survey responses demonstrated that by December of 2016, "[t]he typical large US corporation [was] moving through a data-discovery and assessment phase toward a multi-million-dollar remediation that includes shoring up standard data-privacy and security capabilities in US operations."[14]

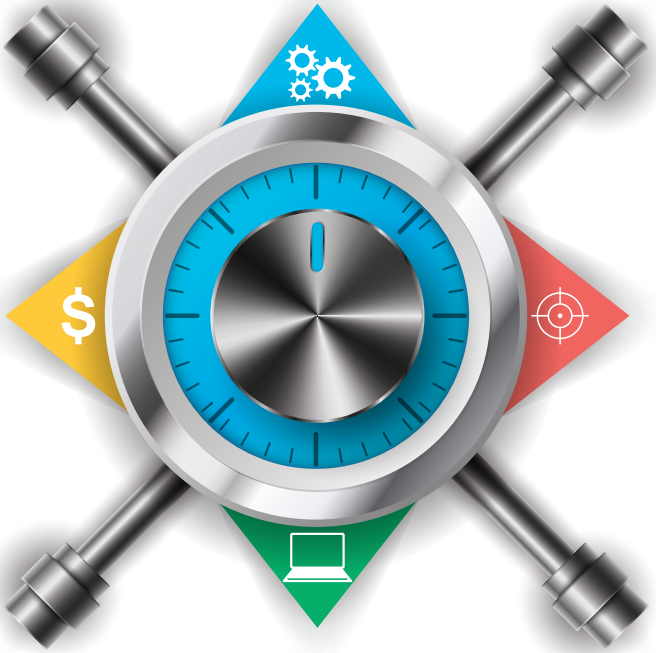
The GDPR is fast approaching, but it is not too late to join other entities in starting preparation. As discussed in the next section, "How Do We Get Ready for the GDPR?," there are steps that entities should begin taking today to prepare to meet their obligations under the GDPR.

[12] *See* PwC, *Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets* ("2016 PwC Study"), https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf. Survey respondents included 200 U.S. C-suite executives from entities with over 500 employees.

[13] *See* 2017 TrustArc Study, *supra*.

[14] *See* 2016 PwC Study, *supra*.

How Do We Get Ready for the GDPR?



Critical First Steps

To prepare for the significant rise in data protection compliance duties coming into effect with the GDPR, entities must remediate their existing internal procedures before May 2018 or risk high fines for their non-compliance. To make this process as simple and straightforward as possible, we recommend undertaking a GDPR "readiness assessment" in the form of a five-step plan, explained below.

Step 1: Gap Analysis and Data Mapping

Entities must first assess their current readiness to meet the many obligations set forth in the GDPR. They must conduct a gap analysis to evaluate their current status of data protection compliance (existing data protection structure), compared with their GDPR obligations (entity GDPR requirements), in these areas: their privacy policies, procedures, processes, and documentation; their people, processes, and technologies; and their data collection, use, storage, sharing, and disposition practices. This stage includes auditing relevant documentation, people, internal processes, technologies, compliance, and training programs. Any non-compliance with the requirements of the EU Data Protection Directive 95/46/EC should also be noted and remedied.

Entities also must ensure that they understand where all EU personal data is stored and their data flows (*i.e.*, transfers of personal data into, within, and outside of the organization). This is typically accomplished through targeted data mapping.

Step 2: Risk Analysis and Phased Risk Remediation Plan

Most entities will be required to make extensive efforts to implement the GDPR requirements, and not all requirements can reasonably be fulfilled at once. Thus, entities must assess which data-processing activities have the highest risk level for their business and the rights of their data subjects, as well as which risks will be the most likely to result in high fines, and tier their priority actions, as well as allocate their resources, accordingly.

Step 3: Project Steering and Resource and Budget Planning

The implementation process requires significant collaboration between an entity, its affiliates, its third-party processors, and its controllers. The process requires education and coordination between the entity's senior management and all of its business units that manage EU personal data. Project responsibilities should be assigned to select personnel in the entity's global headquarters and other key city offices, including the EU offices, and to select an overall, responsible project sponsor and a project manager.

Furthermore, the allocation of the required resources should be carefully planned, in particular concerning internal resources, such as the personnel required for the implementation, legal expenses, and IT expenses (*e.g.*, supporting software, IT audits).

Step 4: Implementation of a Data Protection Structure

To realize the new and extended requirements set out by the GDPR, a strengthened, organizational cross-office data protection management system must be implemented within the entity. This includes defining roles and responsibilities within the involved entities; where relevant, appointing a data protection officer (DPO); implementing concepts, policies, and standard operating procedures (so-called "SOPs") for the GDPR obligations; offering structured and documented employee training pertaining to the obligations and responsibilities deriving from the GDPR; and providing documentation to ensure compliance measures are reviewed and updated regularly. Privacy impact assessments (PIAs) should be documented as should ongoing data-processing activities.

Additionally, a sensible data-processing contract management strategy will have to be implemented because data-processing agreements covering a wide variety of entity processing activities will have to be prepared or updated to comply with the GDPR.

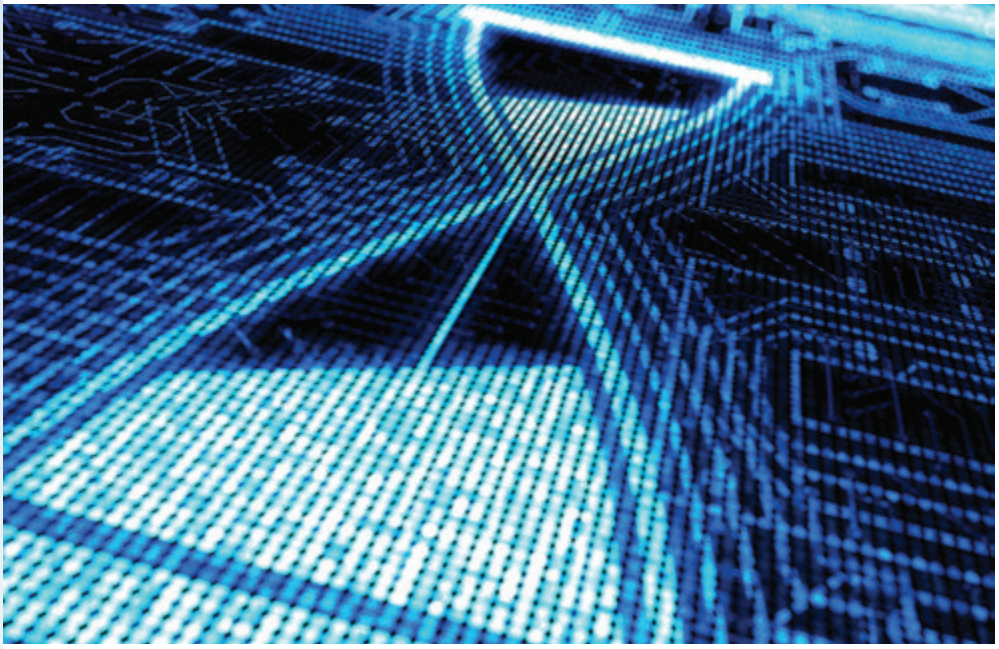
Step 5: Local Add-On Requirements

In addition to the EU-wide GDPR requirements, additional national requirements may very well exist. The GDPR has numerous "opening clauses" that provide EU Member States with discretion to enact additional national regulations. For example, the GDPR allows Member States to enact employment-related requirements that are more restrictive than what is required under the GDPR.

The Global Privacy Challenge

Data privacy is not just an EU issue. Especially for multinational entities, it may well be exceedingly beneficial to use the internal GDPR-compliance restructuring as cause to take a look at non-EU key markets where privacy laws have been updated or strengthened or where policy is heading in that direction. This way, an entity will be able to get a head start on future developments with regard to multinational data privacy laws.

Why Not Just Ignore It?



When examining the costs and benefits of complying with the GDPR, the costs are clear: a GDPR compliance program will divert internal resources away from other valuable projects, creating significant costs, not to mention out-of-pocket expenses for lawyers and consultants. The benefits of launching a compliance program are not easy to quantify. Why not just ignore it?

Non-compliance could result in onerous fines. Many corporations view the GDPR's onerous fines as a key reason for not ignoring the GDPR.[15] Supervisory authorities have asserted their intent to fine entities the maximum amount where appropriate. The following comment from an interview with Helen Dixon, Irish Data Protection Commissioner, is one example that makes this intent clear:

> **Adrian Weckler (AW):** Are you willing to go the full distance in fining companies €20m?
>
> **Helen Dixon (HD):** Yes. We have to be willing to. The legislature in Europe provided for fines up to that level because they believe in certain cases it may arise. Presumably, it would involve many users. But it's absolutely the case that we will be imposing fines against big and small entities based on the issues that come across our desk and the areas of risk we identify. There's nothing surer than this.[16]

---

[15] *See* CIPL, Organisational Readiness for the European Union General Data Protection Regulation, https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/11/cipl_avepoint_gdpr_readiness_survey_report_1107_final-c.pdf (finding, through a survey of multinational companies, that the top senior-management GDPR concern is the "enhanced sanctions regime.").

[16] Adrian Weckler, *Data Protection Boss Vows She Will Use New Powers to Fine Firms Up to €20m*, Independent.IE (27 Apr. 2017), http://www.independent.ie/business/technology/data-protection-boss-vows-she-will-use-new-powers-to-fine-firms-up-to-20m-35657249.html.

General Data Protection Regulation claims will emerge in employment disputes. Entities doing business in Europe are accustomed to complex employment laws, and in some cases, litigious employees and works councils. Unhappy employees and works councils sometimes use data protection non-compliance as a weapon in litigation. If an entity's human resources processes are not compliant with the GDPR, this will significantly weaken the entity's position in employment-related negotiations and disputes. Works councils may even use data protection issues to try to slow down large corporate transactions.

Non-compliance can affect important corporate transactions. Some courts or administrative authorities treat non-compliant data as tainted, and therefore legally unusable. An asset transfer may be deemed null and void, or data may turn out to be unusable for pre-market approval for drugs or medical devices. Tainted data can result in costly legal consequences.

Non-compliance can be a criminal offense. Failure to comply with certain aspects of data protection laws constitutes a criminal offense in some Member States. Most organizations do not want to risk prosecution for criminal violations, even if the risk of prosecution is relatively low. Corporate officers in Europe may also incur personal liability. The GDPR permits class actions, and while civil litigation on data protection is not yet well developed in Europe, consumer bodies are likely to exploit the new litigation avenues opened by the GDPR.

Clients may ask about the GDPR. Many corporate customers are asking their vendors to demonstrate GDPR compliance, or even to sign detailed, data protection addenda to ensure GDPR compliance. A business that has not started its GDPR compliance plan may find itself shut out of important business opportunities.

The GDPR is going global. Another reason to pay attention to the GDPR is that it is becoming a model for many countries around the world. Japan and Korea have relatively new data protection laws inspired in part by the European Union model. Even China's new cybersecurity law has portions that seem directly lifted from the EU playbook. The GDPR may well set the standard for reasonable care for global data protection. For all of these reasons, the GDPR is a good model to use for global data-processing operations.

EU General Data Protection Regulation Preparation Checklist

The EU General Data Protection Regulation (EU GDPR) will come into effect on May 25, 2018. Along with significantly increased penalties (up to 4 percent of annual worldwide turnover), the EU GDPR brings significantly more onerous compliance obligations. Rather than addressing every requisite action item for GDPR compliance, in this checklist, we set forth high-level recommendations for organizations to consider as they prepare to meet their obligations under the EU GDPR. Ultimately, each organization will need to analyze its current GDPR readiness, identify all gaps in its GDPR readiness, and develop and implement a phased action plan for addressing such gaps.

Initial Steps

☐ Appoint Business Owner and Executive Sponsor for Assessing GDPR Readiness

☐ Conduct Personal Data Audit and Develop Phased Compliance Plan

- Analyze Pertinent Policies, Procedures, Standards, Notices, Consents, Contracts, and Other Documentation for Compliance
- Interview Key Persons about Data Privacy and Information Security Processes covering EU Personal Data
- Analyze Types of Personal Data Retained, Role (Controller or Processor), Personal Data Flows, Electronic and Paper Storage Locations, How Personal Data Is Processed and Secured
- Consider Possibilities for Anonymizing and Pseudonymizing Personal Data
- Document Legal Basis for All Personal Data-Processing Activities
- Assess Ability to Secure Personal Data and Address Data Subjects' Rights with Current Technical, Physical, and Organizational Controls
- If Cross-Border Transfers Involved, Confirm Proper Transfer Mechanisms in Place
- Identify Gaps in GDPR Readiness
- Develop Phased Compliance Recommendations
- Estimate Costs to Address Gaps and Obtain Approval for Updated Budget
- Increase Organizational Awareness of Obligations, and Obtain Buy-In for Recommended Action Plan

☐ Prepare Data Map

- Identify Team and Develop Project Plan (Including Whether Targeted or Phased Data Map Is Desired and Data Flow Coverage)
- Review Written Documentation and Conduct Surveys or Interviews
- Prepare Map Covering Storage and Data Flows
- Develop Evergreening Process

Update Data Protection Compliance Program

- ☐ Confirm Necessary People in Place to Lead Program (Including, as Appropriate, Appointment of Data Protection Officer)
- ☐ Update Internal Data Protection Compliance Structure with Cross-Business Unit and Cross-Office Involvement
- ☐ If Applicable, Identify Main Establishment or EU Representative
- ☐ Implement Updated Policies, Procedures, and Processes, Taking into Consideration Specific GDPR Obligations, as well as Data Protection Principles
- ☐ Align Technologies with GDPR Requirements
- ☐ Draft and Implement Policies, Procedures, and Processes for Conducting Risk Assessments and Data Protection Impact Assessments
- ☐ Prepare Templates for Tracking Records of Processing Activities
- ☐ Develop Policies, Procedures, and Processes for Implementing Data Protection by Design and by Default When Creating New Products, Services, or Other Data-Processing Activities
- ☐ Prepare and Implement Policies, Procedures, and Processes for Addressing Data Subjects' Rights (Access, Rectification, Transfer, Erasure, and Objections to Data-Processing Activities)
- ☐ Consider Additional Information Governance and Compliance Initiatives to Reduce Risk of Non-Compliance (*e.g.*, Legacy Information Review and Disposition Projects, Consolidation of Storage Locations, Updates to Cross-Border eDiscovery Processes)
- ☐ Adopt Compliance Monitoring Mechanism
- ☐ Implement a Process for Identifying and Addressing Additional Obligations in Member States, and for Staying on Top of All Pertinent Regulatory Guidance

Recommendations for Enhanced Privacy Notices

- ☐ Review and Update Current Privacy Statements, Notices, and Policies to Cover Additional Details and Meet Other Requirements of GDPR

Recommendations for Addressing Enhanced Consent Requirements

- ☐ Identify Processing Activities Legitimized Through Consents, and Consider Other Options for Legitimizing
- ☐ Revise Consent Language and Mechanisms, as Necessary, to Meet GDPR Requirements
- ☐ Implement Processes to Honor Withdrawals Promptly
- ☐ Analyze Systems for Recording Consent, and Confirm Effective Audit Trail

Data Security Recommendations

- ☐ Assess Current Data Security Measures
- ☐ As Needed, Implement New Technical and Organizational Measures to Protect Personal Data
- ☐ Regularly Test Effectiveness of Technical and Organizational Data Security Measures

Third-Party Vendor and General Contracting Recommendations

- ☐ Prepare Updated Third-Party Vendor Procedures and Checklists
- ☐ Select Only Vendors That Can Implement Necessary Technical and Organizational Security Measures
- ☐ Prepare Addenda to Current Third-Party Vendor Contracts Incorporating Detailed Contractual Requirements
- ☐ Draft Contract Templates for New Vendor Contracts
- ☐ Prepare Addenda and Templates for Agreements with Controllers with Which EU Personal Data Will Be Shared

Cross-Border Transfer Recommendations

- ☐ Thoroughly Analyze Personal Data Flows and Applicable Legal Frameworks
- ☐ Consider Whether Data Flows Could Be Changed to Reduce Compliance Burden
- ☐ Ensure Appropriate Transfer Mechanisms (and Documentation) in Place for All Cross-Border Data Flows
- ☐ If Relying upon Privacy Shield but Not Yet on Privacy Shield List, Take All Actions Necessary to Self-Certify

Data-Breach Notification Recommendations

- ☐ Assess Information Security Measures to Help Ensure Data Breaches Can Be Promptly Detected and Managed
- ☐ Update Data-Breach Incident Management Plan, Prepare Template Notifications
- ☐ Update Processor Contracts to Address Data-Breach Notification Obligations

This checklist has been prepared as a high-level overview of recommendations for GDPR preparation. This checklist is not intended to be an exhaustive list of all GDPR preparation steps.

If you have any questions concerning this checklist or related issues, or if you would like assistance developing policies and procedures for EU GDPR compliance; conducting a Personal Data Audit or a Data Protection Impact Assessment; or addressing your organization's specific compliance challenges in advance of the May 25, 2018, deadline, please contact Laura Clark Fey at (913) 948-6301 or lfey@feyllc.com.

Authors

Laura Clark Fey, Esq., CIPP/E, CIPP/US, CIPM, FIP, leads Fey LLC, a boutique law firm in Kansas City, Missouri, dedicated to helping US and multinational organizations develop and implement solutions to their unique data privacy and information governance challenges. Laura is a member of the Globalization Working Group of the DRI Center for Law and Public Policy, and current chair of the DRI Cybersecurity and Data Privacy Committee's Privacy Specialized Litigation Group.

Susan Gunter, LL.M., is a partner at Dutton Brock LLP, a litigation boutique law firm in Toronto. She is a former member of the DRI Board of Directors (Canada Region) and is the chair of the Globalization Working Group of the DRI Center for Law and Public Policy.

Judy Krieg is a member of the UK law firm of Shepherd and Wedderburn. She specializes in compliance, governance, and financial regulatory matters. She has served as financial regulator (UK Financial Services Authority), Chief Compliance Officer (Rolls-Royce plc), in-house counsel, and external counsel on compliance and investigation matters covering a wide range of industries and involving more than 70 countries. She is member of the Globalization Working Group of the DRI Center for Law and Public Policy.

John Magee, BCL, LL.M., is technology partner with leading Irish law firm William Fry, where he has a particularly strong reputation in the privacy and cybersecurity fields. He is member of the Globalization Working Group of the DRI Center for Law and Public Policy and the International Association of Privacy Professionals. He also sits on the Data Protection & Technology Working Group of the Association of Compliance Officers in Ireland.

Winston Maxwell is a member of the firm of Hogan Lovell in Paris, France. In 2014, he was appointed to the French National Assembly's Commission on Digital Rights, and was asked to contribute to the French Conseil d'Etat's 2014 report on fundamental rights in the digital age. Maxwell has completed projects for the European Commission and the French data protection authority (CNIL) on forward-looking regulatory issues. He is member of the Globalization Working Group of DRI's Center for Law and Public Policy.

Tobias Schelinski is a partner of TaylorWessing, an international law firm with 33 offices in 20 countries. Tobias is based in Hamburg, Germany, and advises national and international clients on privacy law and other tech law related issues. He is member of the Globalization Working Group of the DRI Center for Law and Public Policy.