O'Melveny | What do you want to achieve?

GDPR: Client Toolkit

What is the GDPR?

The General Data Protection Regulation (GDPR) is the E.U.'s new regulation governing the collection, processing, use, and storage of personal data – i.e., almost anything relating to an individual resident in the E.U. that can identify the individual, which includes a broad swath of types of information. Though compliance will largely be self monitored, companies must be able to demonstrate it upon request of E.U. or local authorities. Companies subject to the GDPR must examine their personal data collection and processing practices, and determine what changes they must make in order to comply with the regulation.

THE GDPR IN BRIEF

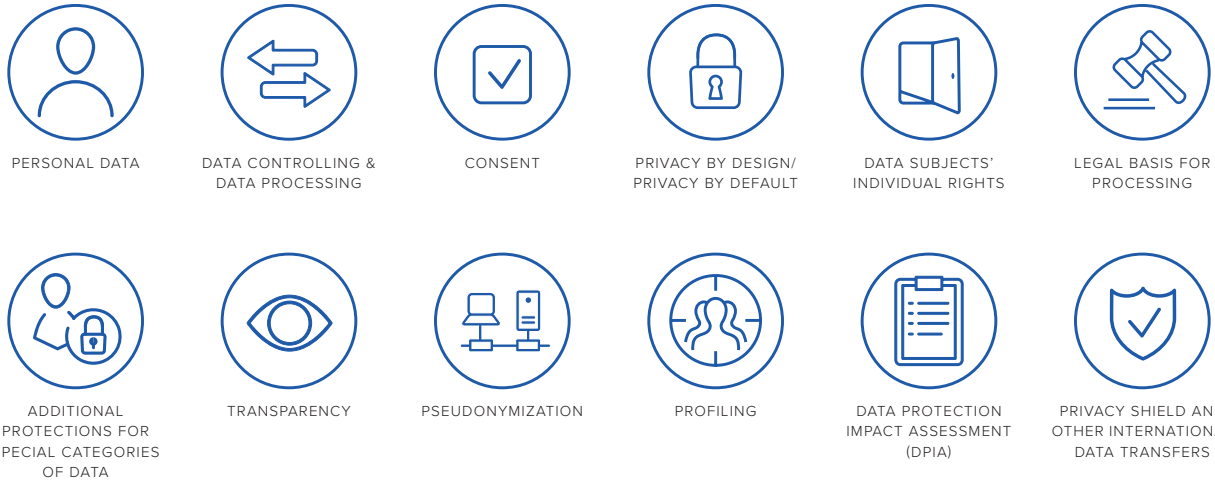
The GDPR replaces the E.U.'s former privacy regime, Directive 95/46/EC (Data Protection Directive or DPD), which was never directly enforceable in E.U. Member States and thus permitted individual countries to develop their own data privacy regimes based on the DPD. The result was varying privacy regulations in E.U. Member States, which made compliance more challenging for companies operating in multiple countries. The GDPR, by contrast, is directly enforceable in all E.U. Member States. Although it permits Member States to adopt national rules in a few limited areas (for instance, to restrict individuals' access to their personal data when it has been collected for scientific, historical, or statistical purposes) the data protection requirements are now more consistent across the E.U.

Although the E.U. is responsible for the GDPR, and E.U. institutions alongside Member State Data Protection Authorities (DPAs) enforce it, the regulation affects not only E.U. companies that process personal data, but also non-E.U. companies that process personal data in connection with offering goods and services to individuals in the E.U., such as websites that are available to E.U. residents and that collect and process those residents' data. It also applies to any companies, regardless of location, that process personal data in the course of monitoring or profiling E.U. residents. As a result, **a company based in the United States, with no operations whatsoever in the E.U., may nonetheless be subject to the GDPR if, for example, the company sells clothing and its goods are available to E.U. residents, and it collects their information as part of its marketing or sales process.**

In addition to its potentially vast reach, **the GDPR imposes significant new substantive requirements that may require companies to transform the way they handle personal data.** Among other things, it requires a "data protection by design" and "privacy by default" approach to companies' development of new systems and products offered to E.U. residents. It also imposes new requirements to notify Data Protection Authorities and affected individuals of data breaches; requires companies to obtain affirmative consent before processing personal data, and explicit consent for particularly sensitive categories of data; and grants individuals new rights with regard to their personal data, including the "right to be forgotten" and the right to correct errors in the data.

In addition, the GDPR provides regulators the power to impose very significant penalties for violations: **violators can be punished by fines as high as €20 million, or four percent of a company's annual worldwide revenue**, whichever is greater, even if worldwide revenue is largely unrelated to the E.U. To mitigate the risk of regulatory enforcement and significant penalties, companies need to ensure they have a robust compliance program.

Though the GDPR retains many concepts from the DPD, it updates them and adds some key new concepts. The following are some of the key concepts incorporated in the GDPR.



Personal Data

- For the most part, the GDPR's definition of personal data or personally identifiable information is the same as the DPD. It includes data elements such as name, identification number, and factors specific to the person such as physical, genetic, economic, or cultural identifiers.
- A couple of new data elements are specified in the new definition: location data and online identifier. These are meant to capture things like IP addresses, mobile phone identifying numbers, and Google IDs, as well as geolocation data. Since this is not data that companies may be used to thinking of as "personal data," companies will need to carefully review how they collect and handle it.

Data Controlling and Data Processing

- The GDPR generally applies to data controllers and data processors. A data controller is a company or organization that determines the purpose and means for the processing of personal data. A data processor processes data on behalf of the controller, though the controller may also process data.
- Data processing is defined under the GDPR as being any operation or set of operations performed on personal data, whether automated or not. The GDPR provides a non-exclusive list of examples of processing, including collection, recording, organization, structuring, storage, retrieval use, and generally making the data available.

Consent

- Under the GDPR, the familiar concept of consent takes on expanded meaning and import. The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." This is a lower standard than the "explicit" consent required for the sensitive categories of data.
- But while "freely given" and "unambiguous" are familiar terms from the DPD, the requirement of "specific" consent adds a new hurdle for companies to comply with the GDPR, and is certainly higher than the standard to which companies in other countries may be accustomed. That is, **companies now cannot use one statement of consent from an individual as a blanket statement to allow all sorts of processing of data collected: rather, consent must be sought for each type of processing, for each purpose for which the company seeks to use the data.**
- **Consent must now also be active.** That is, companies can no longer rely on silence, inaction, or pre-checked boxes. In addition, statements of consent cannot be "bundled" with other statements (such as when the individual is agreeing to the company's terms of use). As a result, **companies can no longer, for example, simply post a link to their privacy policy on their website and expect this to suffice: they must require users to actively accept the terms under which the company will be using their personal data.** Companies will have to review and update their current opt-in procedures. Overall, obtaining effective consent from individuals under the GDPR will require more thought and effort than before.

Privacy by Design/Privacy by Default

- The GDPR embraces the idea of ensuring that privacy is a consideration for companies from the beginning of a product's or service's lifecycle. Rather than considering how to incorporate privacy into a product after it has already been designed, the GDPR requires companies to consider privacy from the outset.
- In addition, under the GDPR regime, companies' default data collection mode must be to gather only the personal data necessary for a specific purpose. **Mass collection of personal data that might someday be useful, or that a company wants just so it can market other products to customers, is not permitted.**

Data Subjects' Individual Rights

- The GDPR introduces several new individual rights for consumers. The one that has received the most attention is the "right to be forgotten," which in practice means that a company must honor a consumer's request to delete information about her if it is "no longer necessary in relation to the purposes for which they were collected or otherwise processed"; if the consumer retracts her consent or objects to the processing and there is no other lawful basis for processing; if the personal data are no longer necessary for the purpose for which they were collected; if the personal data were unlawfully processed; if

the personal data must be erased to comply with a Member State law; or if the personal data were collected in relation to the offer of information society services.

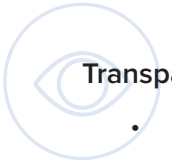
- Other individual rights now enshrined in the GDPR are the right to rectification (correction of personal data), the right to data portability, and the right to object to or restrict processing in certain cases.
- The right to rectification permits data subjects to ask data processors to correct or complete inaccurate personal data "without undue delay."
- With the right to data portability, data subjects who previously consented to processing and whose personal data are being automatically processed can demand the personal data "in a structured, commonly used and machine readable format" so that they can provide it to another data controller.
- Data subjects can also object to processing of their personal data that is being done in the public interest or for a legitimate interest pursued by the controller or a third party, or when the personal data are being processed for purposes of direct marketing, including related profiling.

Legal Basis for Processing

- Companies must now identify a legal basis for any personal data processing that they wish to do. If there is no such basis, the processing is illegal.
- Possible legal bases include consent from the individual; necessity to perform a contract with the individual; compliance with the data controller's legal obligations; vital interests of the individual (in essence, life-or-death situations); necessity for the public interest; and the legitimate interests of the controller, though the rights and freedoms of the individual take precedence over these. In addition, Member States may provide for additional, limited lawful bases for processing that are connected with national law or the public interest.

Additional Protections for Special Categories of Data

- The GDPR slightly expands and further clarifies the types of data, called "sensitive" under the DPD, that require special treatment. Companies handling this kind of data must obtain "explicit" (rather than just "unambiguous") consent, unless the data are in the public sphere or must be processed to protect the individual's "vital interests," among other exceptions.
- Sensitive data includes: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership falls into this category, as well as genetic data, biometric data, data concerning health, and data concerning a natural person's sex life or sexual orientation.
- E.U. Member States are permitted to maintain their own distinct rules for the processing of such data, to a certain extent. For instance, a Member State may permit processing of data for employment use if it is necessary and authorized by the Member State's own law. Member States may also introduce additional conditions and limitations surrounding the use of health data.



Transparency

- The GDPR broadens the notice and transparency requirements that have long existed under the DPD.
- Data controllers must disclose to the data subjects, among other things, the time period for which personal data will be stored; information about international data transfers; and what rights are available to individuals with regard to their personal data, including the right to complain to their data protection authority.

Pseudonymization

- Pseudonymized data are data that has been separated from direct identifiers, so that it cannot be linked directly to a person's identity without the use of additional information that is held separately and protected.
- Because pseudonymization reduces the privacy risks for individuals, the GDPR's requirements are relaxed, though not altogether removed, when companies use this process for personal data that they collect. For example, pseudonymized data can be processed for uses beyond that for which it was originally collected, unlike other personal data. Use of pseudonymized data also helps to show that a company is incorporating the concept of "privacy by design" into its business, as required by the GDPR.

Profiling

- "Profiling" under the GDPR is used to refer to automated processing of people's personal information with the purpose of evaluating personal aspects of those people. Examples of activities that may count as profiling include behavioral marketing, retargeted emails, automated credit offers, or e-recruiting that is done without human intervention. Though some data profiling is still permitted under the GDPR, it is significantly restricted, particularly when it results in effects to individuals' legal rights, and individuals in the E.U. have the specific right to object to the use of their personal data for profiling at any time.

Data Protection Impact Assessment (DPIA)

- If a company expects to process personal data in such a way that it is likely to result in a high risk of harm to individuals' privacy, the GDPR requires the company to first conduct an assessment of what those risks are and how the company's personal data protection framework will be affected. High-risk processing under the GDPR includes automated processing or profiling that results in decisions that affect an individual's legal rights; large-scale processing of special categories of data; and large-scale, systematic monitoring of a public area. Member States may require DPIAs for other types of processing.
- Although some companies already conduct Privacy Impact Assessments (PIA), these are not necessarily interchangeable with DPIAs, since the GDPR outlines specific recordkeeping obligations for DPIAs that a generic PIA may not meet. For instance, while PIAs usually assess data use from the company's perspective, the GDPR requires that DPIAs be done from the point of view of the individual data subject, and should seek the

views of the data subjects. DPIAs also must include additional questions, which are not necessarily in a typical PIA, to show compliance with the GDPR, as well as to operationalize the privacy by design concept. The GDPR also specifies certain documentation and descriptions that must be included in a DPIA.

Privacy Shield and Other International Data Transfers

- The GDPR permits cross-border data sharing only to countries that provide "adequate" protection for personal data—or to companies that are subject either to legally binding corporate rules that satisfy the GDPR's requirements and have been approved by a DPA, or to standard contractual clauses that have been written by the European Commission. Transfers from countries in the E.U. to certain countries with data privacy regimes that have already been judged to be "adequate" are automatically permissible under the GDPR.
- One way for U.S. companies to satisfy the GDPR's "adequacy" requirement is to enroll in the E.U.-U.S. Privacy Shield, which is administered by the U.S. Department of Commerce and requires companies to have compliant privacy policies and certify annually that they will adhere to the Privacy Shield principles. The Privacy Shield will undergo annual review by E.U. and U.S. officials, and some E.U. politicians have raised questions about the Privacy Shield's sufficiency, so it is possible that this option will not survive for companies seeking to transfer data from the E.U. to the U.S., though if it is scrapped it may be replaced, just as the Privacy Shield replaced an earlier scheme that was ruled unlawful by the European Court of Justice.

Companies will need to assess their existing privacy framework and determine whether any changes should be made to comply with the GDPR.

1

Confirm Whether and How the GDPR Applies to Your Company

If you operate within the E.U. or were complying with its predecessor, the DPD, then you likely already know that the GDPR applies to you. But with the GDPR's expanded territorial scope, it reaches companies that were not previously subject to the E.U. law. **Specifically, if your company processes personal data in connection with offering goods and services to individuals in the E.U., or if it processes personal data in the course of monitoring or profiling E.U. citizens, it is subject to the GDPR.** In addition, consider that even if your company does not process E.U. citizens' data, if you are a vendor or supplier to E.U. companies, they may require that you comply with the GDPR. Note that although the United Kingdom is in the process of leaving the E.U., its officials have made clear that its data privacy laws will continue to conform with the standards of the GDPR.

To understand whether you may fit in this category, ask:

- Are you or are any of your subsidiaries or affiliated entities registered as a controller with any Data Protection Authority in the E.U.?
- Do you offer goods or services to individuals in the E.U.?
- Do you have a website that is accessed by E.U. residents and collects any identifying information from them, including about their location?
- Do you monitor the behavior of individuals in the E.U. such as through tracking technologies?
- Do you collect or process personal data from individuals in the E.U. for purposes of (a) offering them goods and services or (b) monitoring their behavior online or on their devices?
- Do you obtain from other entities the personal data of E.U. residents?
- Do you interact with E.U. companies or other companies subject to the GDPR as a vendor or supplier?

2

Advise Key Stakeholders

Meeting the GDPR's requirements may involve significant changes to a company's structure, as well as major expenditures to come into compliance with the regulation. Everyone at the company who is responsible for its personal data handling activities, from the C-suite down to the leads on specific teams, must be made aware of the importance of the GDPR and of the compliance process. The high fines for noncompliance with the GDPR are meant to grab attention for this reason. **Executives must understand that the GDPR is not just a minor IT or privacy/legal regulation, but that it could require fundamental changes in the way the company operates, and, if those changes are not made, could lead to extremely debilitating punishment.**

3

Consider Whether Corporate Structure and Personnel Updates are Needed

Stakeholder buy-in is especially important since even before tackling some of the regulation's finer points, it may be necessary to make some big changes and hires. Most notably, the GDPR requires companies to have a representative in an E.U. Member State if they lack a physical presence in the E.U., unless their personal data processing is only occasional, not on a large scale, not involving special categories of data, and not likely to infringe on data subjects' rights and freedoms with regard to the privacy of their personal data. If your company is subject to the GDPR, then, it will want to consider whether it would better serve its interests to establish a footprint in the E.U. or to identify a suitable representative that can act on its behalf.

The GDPR also requires companies whose "core activities" consist of data processing that requires systematic monitoring of data subjects "on a large scale" to appoint a Data Protection Officer (DPO). If a DPO is required, a company must ensure that the DPO has the qualifications and expertise required by the GDPR and establish a structure under which the DPO can perform the duties and tasks specified in the GDPR. Even more widespread changes or additions to H.R. and I.T. teams and their budgets could also be necessary, as additional or different roles and skills will be relevant for holistic, long-term GDPR compliance than may have been for less intense privacy regimes.

4

Assess and Update Your Privacy and Cybersecurity Infrastructure

Whether or not your company is required to appoint a DPO, you will want to make sure that key personnel are trained on both the GDPR and on the company's use of personal data. In particular, consider training those in the I.T. or information security group; H.R. managers; product development leads, marketing managers; and communications directors. Even in cases where a DPO is not required, additions to a company's privacy team will likely be warranted. Someone in a DPO-like oversight role may be needed to help the company comply with the GDPR and, more generally, to manage overall personal data management practices.

In addition, the GDPR requires companies to engage in ongoing privacy-related activities such as conducting DPIAs and responding to requests from individuals concerning their personal data. Staff will also have to handle new technical demands imposed by the law, such as being able to delete information in response to a request to be forgotten or rectify information that is identified as inaccurate. As a result, unless your existing privacy infrastructure is already

robust enough to handle the addition of these new obligations, **you should consider making additional hires or reallocating and training existing staff to handle GDPR compliance.**

5

Engage in Comprehensive Data Mapping

Before you can determine what changes need to be made to your company's data protection procedures, you need to know exactly what kinds of personal data you are collecting and what the handling procedures currently are. Once there is a clear understanding of what kind of personal data are at issue, you will be able to determine what requirements in the GDPR apply. In general, but especially for GDPR purposes, data mapping will involve asking both how personal data are collected and how it is processed, stored, and shared. The GDPR governs companies' interaction with individuals' personal data at each step in the lifecycle, so it is important not to overlook any of these pieces.

When it comes to understanding the personal data you collect, the following questions are among the most critical:

- What elements of personal data are being gathered?
- For what purpose is the company collecting the personal data, and is it collecting the minimum amount of data necessary to meet that stated purpose?
- What level of consent has been sought from the customer or user?
- Is any "sensitive" personal data being collected, such as health records or financial information?
- Is the company collecting any data from children (generally, minors under 16 years of age, though individual jurisdictions may enact laws permitting wider collection for minors over age 13)?

After gaining this basic knowledge about the universe of data that your company collects, you must assess how that data are being processed and stored. Restrictions on, and oversight of, data processing are at the heart of the GDPR. To comply with these new restrictions, you should understand, among other things:

- where and how personal data are being stored (in terms of types of servers or other hosts, outside vendors, geographic location, etc.);
- how the personal data are being protected (whether it is encrypted, anonymized or pseudonymized, and who has access to it);
- how and why the personal data are being processed;
- how long the personal data are maintained;
- whether the personal data are used in profiling or other automated decision-making processes;
- to what third parties (including vendors) is the personal data disclosed, and in what circumstances; and
- what internal records are kept of these processes.

6

Conduct a Gap Analysis

Based on your data map, you should now review your personal data handling practices and procedures compared to those set forth in the GDPR. The GDPR, while new and sweeping in scope, builds extensively on the prior DPD that applied in the E.U., as well as on data protection concepts from elsewhere in the world, so unless your business has never complied with any kind of data privacy law, it is unlikely that this gap analysis will reveal that every requirement in the GDPR is something new that the company must consider and implement. Rather, there are likely to be specific areas where the company's past practices do not match up to the new expectations set forth in the GDPR and will need to be modified.

7

Set Priorities Based on Gaps Discovered

After the gap analysis is complete, you can set priorities for coming into compliance with the GDPR. These priorities will depend on the extent to which your company operates in the E.U. or has European customers, as well as the amount and type of personal data your company is handling. If you have determined that your company is subject to the GDPR, it will obviously need to reach compliance one way or another, but companies with less of a presence in Europe may determine that certain areas of compliance are more immediately important. These priorities may also be informed by other considerations, such as the company's I.T. budget and priorities (e.g. the need to update the company's cybersecurity). Moving forward to implementation, the priorities list should be used for planning which changes and updates should be handled first.

8

Develop an Implementation Plan

Although it is important to make sure the priorities are kept at the top of the work list, at the same time it can be helpful to address some more minor issues first to make sure things are getting accomplished. The implementation plan should be periodically reviewed and updated to respond to issues and developments that arise during implementation. Above all, the implementation plan should ensure that the company keeps in motion on the path to compliance.

9

Educate Employees and Customers

For the implementation plan to work, a company's employees must be integrally involved in and supportive of the compliance process. This should include training and education on the basic principles of the GDPR and the procedures being implemented by the company for compliance. In particular, to the extent that they do not already, employees should understand the importance of data protection and privacy. To the extent employees are not already trained on these subjects, the GDPR provides a helpful avenue for orienting them to the issues. You should also consider educating your customers in the same way. The GDPR grants individuals several rights with regard to their personal data (right to portability, right to be forgotten, etc.). Providing customers with key information about those rights assists both in fulfilling the GDPR's aim of transparency regarding personal data, and in ensuring that when customers exercise those rights, they do so in a way that works with your company's internal processes. You could consider incorporating this information into an updated privacy policy, a blog post or video, or by separate email to customers, among other possible methods.

10

Begin Utilizing Principles of Privacy by Design/Privacy by Default

The GDPR requires that privacy be the default setting for companies when they are handling E.U. individuals' personal information. **When designing products or setting up services, privacy concepts must be built in to their architecture, rather than being an afterthought or a one-time process.** In Europe, some e-petitions, electronic toll road pricing systems, and smart metering programs have been designed in this way. Privacy considerations will need to be a fundamental part of the product design and development process, which is a significant new obligation. Companies will need to develop and document protocols for satisfying this requirement.

11

Create a System for Monitoring Data Handling and Demonstrating Compliance

Not only does the GDPR establish certain requirements for recordkeeping, but as a matter of good practice for potential future litigation and regulatory actions, keeping proper records is essential. Under the E.U.'s previous data protection regime, data controllers, or their representatives in Europe, were required to register their data processing activities with the relevant DPA. Under the GDPR, companies no longer need to notify DPAs of their processing activities, but are required to document their activities internally, and to maintain and continually update the record so that it can be provided to DPAs on request. Specifically, records that must be maintained include records of consent from data subjects, records of processing activities under the company's responsibility, and documented processes for protecting personal data (e.g. information security policy, encryption policy, etc.).

12

Continually Reassess and Confirm Compliance While Implementing Compliance Plans and At All Times Afterwards

The compliance process will not necessarily be linear, and will require periodic and frequent review and updating to ensure that the company is on track to comply with the GDPR and, after attaining compliance, maintains that status.

KEY CONTACTS

Lisa Monaco

lmonaco@omm.com
+1 202 383 5413
Washington, DC

John Dermody

jdermody@omm.com
+1 202 383 5306
Washington, DC

Scott Pink

spink@omm.com
+1 650 473 2629
Silicon Valley

Christian Peeters

cpeeters@omm.com
+32 2 642 41 32
Brussels

Randall Edwards

redwards@omm.com
+1 415 984 8716
San Francisco

ABOUT O'MELVENY

It's more than what you do: it's how you do it.

Across sectors and borders, in board rooms and courtrooms, we measure our success by yours.

And in our interactions, we commit to making your O'Melveny experience as satisfying as the outcomes we help you achieve.

Our greatest accomplishment is ensuring that you never have to choose between premier lawyering and exceptional service.

So, tell us. What do you want to achieve?

Century City • Los Angeles • Newport Beach • New York • San Francisco • Silicon Valley • Washington, DC
Beijing • Brussels • Hong Kong • London • Seoul • Shanghai • Singapore • Tokyo

omm.com