Two Years of GDPR: What We Have Learned and What You Need to Know

VORYS

Introduction

The European Union's General Data Protection Regulation (GDPR) became effective in May 2018. Press coverage in the United States largely focused on the eye-popping maximum penalty for certain violations: as much as the ***greater of*** €20 million or 4% of gross annual turnover. Almost two years after GDPR became effective, however, many US businesses remain uncertain whether GDPR applies to them at all, and if it does, what compliance entails. Too often, companies have been quick to assume that GDPR has no applicability to them because they have no facilities within the European Union, or that they can achieve compliance through the simple expedient of tweaking an existing consumer privacy notice on their websites.

Of course books can be—and have been—written on the full scope of GDPR, and the truth is that, given the relative newness of the law, uncertainty remains considering precisely how the relevant regulators (called "supervisory authorities" in GDPR) in each EU member state will interpret and apply several of its provisions. Nonetheless, this paper offers some general guidance concerning some of the larger issues any US company should consider when deciding whether, and how, to attempt to comply with GDPR. Further, as states like California adopt new statutory schemes that bear similarities to GDPR, and as the US Congress hears more calls for comprehensive privacy regulation in the United States, all US businesses that handle personal data—including the data of their employees, in addition to that of their customers—should consider the possibility that GDPR-like privacy principles may become relevant to their operations in the future.

General Overview

KEY DEFINITIONS

Understanding GDPR starts with understanding its definition of certain key terms, whose meaning may not be apparent to a US business familiar with privacy regulations only in the United States. Here are the most important:

Personal Data: Any information relating to an identified or identifiable natural person.

Identifiable Natural Person: A natural person 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.

Processing. Any operation or set of operations that 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 of combination, restriction, erasure or destruction.

Controller. The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

Processor. A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Consent. 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.

Psuedonymization. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Profiling. Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects related to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

The first two of these definitions in particular broaden the scope of privacy regulation far beyond that to which most US businesses are usually subject. "Personal data" is any information relating to an identifiable natural person, and an "identifiable natural person" is one who ***can be*** identified, ***directly or indirectly***. An IP address, for example, may well satisfy this definition, because it is likely possible, at least indirectly, to identify the owner of the IP address (although this assumes that the "data subject" using a connection with a specified IP address is in fact the owner of that IP address).

AN OVERVIEW OF GENERAL GDPR CONCEPTS

The European conception of privacy regulation differs significantly from that prevalent in the United States. Several concepts underlying GDPR demonstrate this, and these concepts pervade the regulation.

First, the GDPR envisions privacy as a fundamental human right. This is quite different from the approach in the United States, which typically

TOO OFTEN, COMPANIES HAVE BEEN QUICK TO ASSUME THAT GDPR HAS NO APPLICABILITY TO THEM BECAUSE THEY HAVE NO FACILITIES WITHIN THE EUROPEAN UNION, OR THAT THEY CAN ACHIEVE COMPLIANCE THROUGH THE SIMPLE EXPEDIENT OF TWEAKING AN EXISTING CONSUMER PRIVACY NOTICE ON THEIR WEBSITES.

asks whether the data subject has a "reasonable expectation" of privacy.[1] This is particularly apparent in the employer-employee relationship. In general, in the US, an employee's emails, written during the scope of employment and using the employer's systems, belong to the employer; there is little controversy about this, with disputes arising only around whether the email was actually written in the scope of employment or whether personal emails sent and received over company resources are also company property. In the EU, by contrast, an employee's email will contain information that will likely satisfy the definition of "personal data" even where that email was sent or received in furtherance of the employee's job duties. An email address, of course, is information about a natural person, and if coupled with the employee's name it is information about an identified natural person; consequently, it is "personal data" and the employee is a "data subject," regardless of why the employee sent the email or who owns the server from which it was sent and on which it is stored.

Second, the concept of "consent" embodied in GDPR is far more protective of the data subject than it is in the US. Where it requires consent, the GDPR requires that consent be specific and informed, freely given, and the result of an affirmative act or statement. Consent by failing to "opt out" is not consent as defined under GDPR. With the exception of certain industry or sector specific statutes or regulations, the US approach is quite different. Many US websites, for example, feature privacy statements with language along the lines of "by using this website, you consent to our use of the data we collect;" perhaps they also offer the user an opportunity to "opt out" of certain uses of their data by checking a box labeled "I decline." This form of "passive" consent will not pass muster under GDPR.

Third, GDPR requires that all processing activities—including collection of personal data, any use of it, and any transfer of it—have a specific "lawful basis." Consent is one such basis, but where consent is not required, the processing activities must be in furtherance of some other specific lawful basis permitted by the regulation. Importantly, merely furthering the data controller's or data processor's unspecified "business interests" will often not be sufficient. One use of personal data that is common in the United States may be quite problematic under GDPR: the sale of consumer data to third parties for their marketing purposes. Merely disclosing to a data subject that this sale may occur does not satisfy the requirement that the controller selling the data has a lawful basis to do so.

---

[1] The US Constitution, for example, never uses the word "privacy," and the word "private" appears only in the Fifth Amendment (regarding taking private property for public use). The Fourth Amendment—which is sometimes thought of as a source of a right to privacy—secures the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." Like all rights protected by the Constitution, this is a right only against government action; one has no Constitutional "right" to be free from "unreasonable searches" conducted by businesses.

Finally, the GDPR purports to apply extraterritorially, extending its reach even to US-based businesses with no physical presence anywhere within the EU. This provision, coupled with the enormity of the potential fines a regulator could impose, has caused both alarm and confusion in the US, resulting in something of a paradox: some US companies are resting in the false sense of security created by the belief that GDPR cannot reach them because they do not operate in the EU, while others, to whom the extraterritoriality provisions may not apply, expend needless resources attempting to comply with the regulation.

The Extraterritorial Reach

GDPR Article 3 sets out the extraterritorial scope of GDPR. The article provides:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

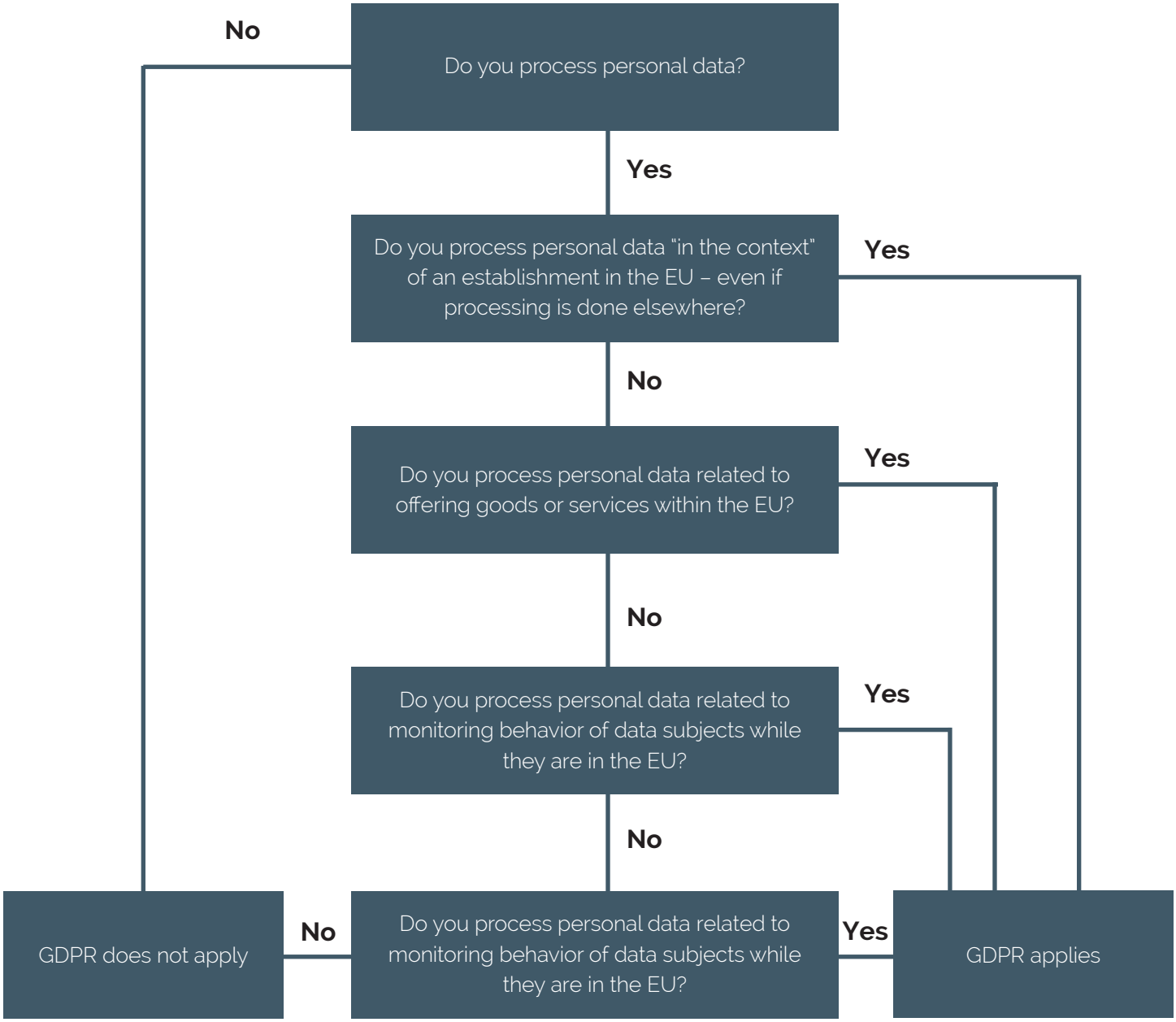
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behavior as far as their behavior takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

GDPR PURPORTS TO APPLY EXTRATERRITORIALLY, EXTENDING ITS REACH EVEN TO US-BASED BUSINESSES WITH NO PHYSICAL PRESENCE ANYWHERE WITHIN THE EU.


Do you process personal data?
No
Yes
Do you process personal data "in the context" of an establishment in the EU – even if processing is done elsewhere?
Yes
No
Do you process personal data related to offering goods or services within the EU?
Yes
No
Do you process personal data related to monitoring behavior of data subjects while they are in the EU?
Yes
No
GDPR does not apply
No
Do you process personal data related to monitoring behavior of data subjects while they are in the EU?
Yes
GDPR applies

VORYS

Two features of this provision often cause confusion.[2] First, Article 3(1) is not limited to the processing of personal data of data subjects within the EU; the section reaches any processing activities that take place within the EU, even if the data subjects are located outside the EU. It would, for example, apply to processing activities regarding US citizens if the processing is done within the EU. Second, Article 3(2)(a) applies even to a US-based business that has no physical presence within the EU if that business is processing personal data in connection with offering goods or services within the EU. For example, a retailer operating a web site that is accessible from the EU, that receives orders from within the EU and that fulfills those orders by sending goods to EU addresses, is subject to the provision. That same retailer, by contrast, is not subject to the GDPR merely because it collects personal data from a shopper at one of its US-based brick and mortar stores, even if that shopper happens to be a EU citizen, although if the retailer then uses that personal data to market to the EU citizen once she has returned to the EU that processing activity would likely be within the regulation's scope.

The scope of Article 3(2)(b) also sometimes surprises US-based businesses. It applies, for example, to monitoring of employee behavior when that behavior takes place within the EU. In fact, as written, the provision may be broad enough to apply to a US business monitoring its US-based employee's activities while that employee is traveling, on the job, within the EU.

General Principles Of Processing

GDPR lays out general principles governing the processing of personal data. It must be:

1. processed lawfully, fairly and in a transparent manner (the lawfulness, fairness and transparency" principle);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes (the "purpose limitation" principle);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the "data minimization" principle);
4. accurate and "where necessary" kept up to date (the "accuracy" principle)

---

[2] A separate question is whether, and how, a European regulator or private citizen could enforce GDPR against a US business. If the business has a physical location within the EU, it may well be that a EU court or regulator could assert personal jurisdiction over that business. If, however, the US-based business has no physical location within the EU, there are serious questions regarding how a EU regulator or court could reach that US business and whether a US court would cooperate with any attempt by a regulator or private litigant to collect a fine or judgment imposed in the EU. The answers to those questions are complex, and beyond the scope of this white paper.

5. 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 (the "storage limitation" principle.

6. 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 (the "integrity and confidentiality" principle).

The regulation adds an additional "accountability" principle: the controller "shall be responsible for, and be able to demonstrate compliance with," each of the previous principles. Most of the rights the GDPR provides to data subjects, and the obligations it imposes on controllers and/or processors, are in furtherance of one or more of these principles.

The regulation provides only specific lawful purposes for processing; processing that is not done in furtherance of one of these specific purposes is unlawful. Processing is lawful where:

1. the data subject gives consent to processing for specific purposes;

2. it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering a contract;

3. it is necessary for compliance with a legal obligation to which the controller is subject;

4. it is necessary in order to protect the vital interests of the data subject or of another natural person;

5. it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. it is necessary for the purposes of the "legitimate interests" pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Where a controller or processor intends to rely on consent, the controller "shall be able to demonstrate that the data subject has consented." Any written consent that is included in a writing that contains other information must be clearly distinguishable from the other contents, must be intelligible and easily accessible, and must use clear and plain language. The data subject must have the right to withdraw consent to any further processing at any time, and the controller must inform the data subject of that right before the data subject provides consent. Importantly, "[i]t must be as easy to withdraw consent as to give it." This last point is a potential stumbling block; if a data subject can provide consent simply by checking a box on a website, she must be able to withdraw consent as easily. This

IF A DATA SUBJECT CAN PROVIDE CONSENT SIMPLY BY CHECKING A BOX ON A WEBSITE, SHE MUST BE ABLE TO WITHDRAW CONSENT AS EASILY. THIS MAY POSE A TECHNOLOGICAL DIFFICULTY FOR MANY BUSINESSES, WHICH MAY BE FORCED TO REASSESS HOW THEY SECURE CONSENT IF THEY CANNOT PROCESS WITHDRAWALS OF IT AS EASILY.

may pose a technological difficulty for many businesses, which may be forced to reassess how they secure consent if they cannot process withdrawals of it as easily as they had initially planned to process grants of consent. Whether consent is truly "free" is also of specific concern to the Regulation, which directs the controller to take "utmost account" of whether the "performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

Businesses intending to use personal data for marketing purposes, or to sell it to third parties, may be tempted to conclude that marketing is a "legitimate interest" within the meaning of the regulation. That may be a mistake. The official commentary to the GDPR, in the form of the Recitals, appears to be of two minds on the subject. Recital 47 states, in part, "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." At the same time, Recital 70 implies that direct marketing is subject to the data subject's consent, at least in the form of a right to object and in the form of an advance notice to the data subject: "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information." Other commentary, while not "official," urges against interpreting the lawful basis prohibitions to include "open-ended" exceptions, and particularly calls out the "legitimate interest" exception as deserving a narrow interpretation.[3] Businesses planning to use personal data for direct marketing should be cautious if they have not secured the data subject's prior consent, and it is likely that the "legitimate interest" basis would not support the sale of personal data to a third party in any event.

GDPR imposes additional restrictions on the processing of personal data related to children under 16 (or younger, if a member state chooses, so long as the restriction applies to a child below 13 years old). GDPR also prohibits the processing of "special categories" of personal data, absent explicit consent or other specific circumstances. "Special categories" of data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. They also include genetic data, biometric 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.

---

[3] Article 29 Data Protection Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (commentary on predecessor to GDPR and then-proposed version of GDPR). The WP29 was formed under a prior data privacy regulation and has subsequently been replaced by the European Data Protection Board. While its guidelines are not binding authority, they do provide insight into how regulators interpret GDPR.

Specific Rights Of The Data Subject

GDPR grants specific rights to data subjects. This paper summarizes them; the full extent of these rights, and how a controller and/or processor must comply with them, merits more discussion than this overview permits.

The Right To Transparency

Information to which the data subject is entitled must be provided in a "concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

Information must be provided in writing, or electronically where appropriate, unless the data subject asks for it to be provided orally and the identity of the data subject is proven.

The controller must provide information free of charge, unless the information request is "manifestly unfounded or excessive."

The controller must provide certain information within one month of the request, subject to certain extensions.

If the controller does not intend to provide the requested information, it must tell the data subject why and must tell the data subject she has the right to lodge a complaint with a supervisory authority and to seek judicial relief.

The Right To Information Obtained From Or About A Data Subject

The controller must provide specific information to a data subject when the controller obtains personal data from the data subject. With certain exceptions, the controller must provide specific information to a data subject within no more than one month of receipt when the controller receives personal data from a source other than the data subject, or at the time the personal data is first used to contact the data subject or first disclosed to a third party.

Information That Must Be Disclosed to Data Subject

	Personal Data **Directly** Obtained from Data Subject	Personal Data **Not Directly** Obtained from Data Subject
	When should the information be provided?	
	At the time when personal data are obtained	Within a reasonable period after obtaining the personal data, but at the latest, one month or when personal data are first used to communicate with data subject or first dis-closed to a third party
	What information must be supplied?	
Identity and contact details of the controller	Yes	Yes
Contact details of data protection officer	Yes	Yes
Purposes and legal basis of the processing, in-cluding the legitimate interests that justify pro-cessing where the controller relies on that lawful basis	Yes	Yes
Recipients of the personal data	Yes	Yes
Fact that the controller intends to transfer per-sonal data abroad, with additional disclosures if so	Yes	Yes
Categories of personal data concerned	No	Yes
Period for which the personal data will be stored	Yes	Yes
Right to request access, rectification, or erasure of personal data	Yes	Yes
Right to withdraw consent	Yes	Yes
Right to lodge complaint with supervisory au-thority	Yes	Yes
From which source the personal data originate	No	Yes
Whether provision of personal data is a statuto-ry or contractual requirement, with disclosure of possible consequences to data subject of failing to provide personal data	Yes	No
Existence of automated decision-making	Yes	Yes
Intent to further process personal data for pur-pose other than for which it was collected	Yes	Yes

The Right To Access

Data subjects have the right to obtain from the controller confirmation as to whether personal data concerning them are being processed, access to the personal data, and most of the information in the table above.

If personal data are being transferred to a recipient in a third country, the "appropriate safeguards" in place relating to the transfer.

Controllers must provide a copy of the personal data undergoing processing when requested by a data subject. If the data subject requests the copy electronically, the controller is to provide the copy using "a commonly used electronic form." The controller must provide the copy free of charge the first time the data subject requests it; the controller can charge a "reasonable fee based on administrative costs" for further copies.

The Right To Rectification

The data subject has the right to have inaccurate personal data corrected by the controller.

The Right Of Erasure (often called the "right to be forgotten")

Data subjects have the right to demand that the controller erase their personal data under specific circumstances:

- the personal data are no longer necessary in relation to the purposes for which they were collected
- the individual withdraws consent
- the individual objects to the processing and there are no overriding legitimate grounds for the processing
- the personal data have been unlawfully processed
- the personal data have to be erased for compliance with a legal obligation

The personal data must be deleted without "undue delay." Some exceptions to this requirement exist, such as where the personal data is necessary to the controller's assertion or defense of legal claims.

The Right To Restriction Of Processing

Data subjects have the right to restrict the controller from processing personal data. Controllers must restrict the processing of personal data in the following instances:

- the accuracy of the personal data is contested by the individual
- the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead

- the controller no longer needs the personal data for the purposes of the processing, but the data subject requires the personal data for the establishment, exercise or defense of legal claims
- the data subject has exercised a right to object to processing, and the restriction is requested while the controller verifies whether it has legitimate grounds for the processing that override the data subject's objections

Although continued processing is restricted if the data subject exercises this right, controllers may continue to store the personal data.

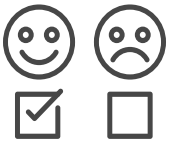
The Right To Data Portability

Data subjects have the right to receive the personal data concerning them "in a structured, commonly used, and machine-readable format," and to transmit those data to another controller without hindrance. Controllers are obligated under this right where the processing is based on consent, and where the processing is carried out by automated means. Upon request by an individual, and where technically feasible, controllers must transmit the personal data directly from one controller to another.

The Right To Object

Data subjects have the right to object to processing of their data for certain purposes. Of central interest to US businesses is the right to object to processing for direct marketing purposes, including to any profiling that is related to that direct marketing. If the data subject does object to processing for direct marketing purposes, that processing must cease. The controller, "[a]t the latest at the time of the first communication with the data subject," must explicitly bring the right to object to processing to the data subject's attention, and that right must be presented "clearly and separately from any other information."

The Right Not To Be Subject To Automated Individual Decision-Making, Including Profiling



Uniquely among the other express rights, the right discussed here does not require any act by the data subject; it is better understood as a prohibition on subjecting data subjects to "a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." This restriction does not apply if the decision is:

- necessary for entering into, or for the performance of, a contract between the data subject and a data controller

- authorized by EU or member state law to which the controller is subject, and which provides "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests"
- is based on the data subject's explicit consent.

Even where the first and third exceptions apply, "the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

Obligations Of Controllers And Processors

GDPR imposes specific obligations on controllers and processors apart from requiring them to comply with data subjects' rights. Some of these obligations apply specifically only to controllers or only to processors, but others apply to both. As with the discussion regarding data subjects' rights, a full discussion of these obligations is not possible here, but a general overview of them is provided in this paper.

The Obligation to Ensure and to Demonstrate Compliance

- The controller is obligated to "implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in compliance with" GDPR
- "Where appropriate in relation to processing activities," the controller must include in those measures "the implementation of appropriate data protection policies."

The Obligation Of Privacy By Design And Default

"Privacy by design" and "privacy by default" are related concepts. The notion is that, before engaging in a business activity or while developing a product that involves the use of personal data, the business should plan for the protection of data and the minimization of any impact on privacy. As implemented through GDPR, these concepts take the shape set out here:

- At the time the controller determines the "means of processing" and when processing actually begins, the controller must "implement appropriate technical and organizational measures", such as psuedonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of [GDPR] and protect the rights of data subjects.

- Data minimization is an essential component of GDPR's approach to privacy by default. The controller is obligated to ensure that "by default" "only personal data which are necessary for each specific purpose of the processing are processed." GDPR applies this obligation to the amount of personal data collected, the extent of processing of that data, the period for which that data is stored, and who has access to that data.
- Access control is an additional key component. Controllers are to "ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."
- These obligations are all subject to feasibility. As the GDPR puts it, a controller should take "into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing."

The Obligation To Secure Representation Within The EU

When a controller is subject to GDPR by virtue of Article 3(2)—in other words, when it has no physical presence within the EU but either processes personal data of EU data subjects related to offering goods and services to those data subjects while they are in the EU or processes personal data of EU data subjects related to monitoring their behavior while they are in the EU—the controller must designate a representative within the EU. The representative is to be addressed in addition to, or instead of, the controller or the processor by supervisory authorities and by data subjects on all issues related to processing. This requirement is sometimes confused with the obligation to appoint a Data Protection Officer—described later in this paper—but it is distinct.

Some exceptions to this obligation exist. The controller need not designate a representative where all of the following are true:

- The processing is occasional
- The processing does not include, "on a large scale," processing of "special categories" of data (described earlier) or of data relating to criminal convictions or offenses
- The processing is unlikely to result in a risk to the rights and freedoms of natural persons, "taking into account the nature, context, scope and purposes of the processing."

Obligations Related To The Controller-Processor Relationship

It is, of course, possible that the controller is also the processor. Where that is not the case, GDPR imposes requirements on the relationship between the controller and processor. Given the scope of the definition of "processing," this can be a serious pitfall for unwary businesses. Nearly

any vendor or service provider who has access to personal data held by a controller may be considered a "processor." Among these requirements are:

- Controllers are to use only processors "providing sufficient guarantees" that they will "implement appropriate technical and organizational measures" to ensure that processing complies with GDPR and protects data subjects' rights.
- A processor cannot engage another processor without the express written approval of the controller.
- The controller and processor must ordinarily enter a written contract that requires that the processor:
    - Processes personal data only on the controller's documented instructions
    - Ensures that persons authorized to process the personal data are under a duty of confidentiality
    - Takes the required data security measures (described later)
    - Assists the controller "insofar as this is possible" in the controller's efforts to respond to data subjects' requests to exercise their rights
    - Assists the controller in the controller's exercise of certain of its obligations
    - Deletes or returns to the controller all personal data at the end of the processor's provision of services
    - Makes available to the controller all information the controller needs to demonstrate compliance

The Obligation To Maintain Records Of Processing Activities

Controllers must maintain records of processing activities that contain:

- The name and contact information for the controller, any joint controller, any controller's EU representative, and any Data Protection Officer
- The purposes for the processing
- A description of the categories of data subjects and the categories of personal data
- The categories of recipients to whom personal data has been or will be disclosed, as well as any recipients in third countries or international organizations
- Any transfers of personal data to a third country or international organization, and if the transfer is to certain countries (including the US), documentation of appropriate safeguards (described later in this paper)

- "Where possible," the expected time limits for erasure of the different categories of data
- "Where possible," a general description of the technical and organizational security measures taken

The Obligation To Implement Security Controls

GDPR instructs controllers and processors to implement "appropriate technical and organizational measures" to ensure "a level of security appropriate to the risk," after taking "into account the state of the art, the costs of implementation and the nature, scope context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." This rather vague instruction offers scant guidance on the lengths to which a controller or processor must go to ensure an "appropriate" level of security. The Regulation contemplates a cost-risk-benefit analysis, but provides little assurance to a controller or processor that, in the event of a security breach, it will be found to have engaged in that analysis appropriately. GDPR does provide some guidance, and suggests certain measures "as appropriate":

- Pseudonymization and encryption of personal data
- "The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"
- The ability to restore access to personal data "in a timely manner" in the event of an incident
- Regularly testing, assessing and evaluating the effectiveness of security measures

Some industry certifications can serve as "an element" of demonstrating compliance with this obligation.

Obligations In The Event Of A Breach

All 50 states in the United States have some form of data breach notification law, so the concept of a legal requirement to report a breach is not unique to GDPR. The Regulation, however, has specific features that are unique. Processors must notify controllers of a personal data breach "without undue delay," although that phrase is not defined. Controllers, by contrast, must notify the relevant supervisory authority "where feasible" ***not later than 72 hours*** after becoming aware of the breach, unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." Again, GDPR provides no guidance on the scope of the "where feasible" qualification. The notification must provide specific, detailed information about the breach. The controller must also document the breach, its effects and the remedial action the controller takes, so that the supervisory authority can verify compliance with the requirements.

ALL 50 STATES IN THE UNITED STATES HAVE SOME FORM OF DATA BREACH NOTIFICATION LAW, SO THE CONCEPT OF A LEGAL REQUIREMENT TO REPORT A BREACH IS NOT UNIQUE TO GDPR. THE REGULATION, HOWEVER, HAS SPECIFIC FEATURES THAT ARE UNIQUE.

Controllers must also notify individual data subjects of breaches, again "without undue delay," if the breach "is likely to result in a high risk to the rights and freedoms of natural persons," subject to certain exceptions.

For a US business confronted with a potential breach, these provisions are rife with rather vague commands and exceptions; choosing among them is likely to be fraught. As is true with state-side cybersecurity and data breach planning, prudent companies will prepare response teams and response strategies well in advance of having to activate them.

The Obligation To Conduct A Data Protection Impact Assessment And To Consult With Supervisory Authorities

Consistent with its embrace of "privacy by design" principles, GDPR requires that a controller conduct a Data Protection Impact Assessment (DPIA) when a processing activity it plans to take "is likely to result in a high risk to the rights and freedoms of natural persons." This is particularly true where the envisaged processing uses "new technologies." It is also required in certain types of "automated processing" that will result in profiling or decision-making, or in processing on a large scale" of the "special categories" of personal data discussed earlier. The DPIA must include specific elements.

If the DPIA reveals that processing would "result in a high risk in the absence of measures taken by the controller to mitigate the risk," the controller must consult with the relevant supervisory authority before beginning processing. The consultation must include, among other things, the DPIA. If the supervisory authority is not satisfied that the controller has taken sufficient steps to mitigate the risk, it can order the controller not to undertake it.

The Obligation To Appoint A Data Protection Officer

GDPR creates a specific job function for controllers and processors and, under certain circumstances, requires them to hire a person into that function. The decision whether to appoint a Data Protection Officer (DPO) can present a Hobson's choice for a US business: failure to do so when it is required violates GDPR, but appointing one where it is not required could supply a EU court or supervisory authority with personal jurisdiction over a US business that otherwise is absent from the EU.

When Must A DPO Be Appointed?

Controllers and processors must designate a DPO where

- the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of individuals on a large scale; or
- the core activities of the controller or processor consist of processing sensitive personal data on a large scale.

If both the controller and processor determine that a DPO must be designated for their organizations, they may appoint a single DPO so long as she is easily accessible from each establishment. If an organization is not specifically required to appoint a DPO, it may still find it useful voluntarily to designate a DPO. If an organization is unsure as to whether a DPO should be appointed, and decides not to designate a DPO, the Article 29 Data Protection Working Party (the "WP29")[4] recommends that controllers and processors document their analysis. As part of the analysis, organizations should look at their core activities, whether processing takes place on a large scale, and whether the activities are regular and systematic.

"Core activities" relate to the "primary activities and do not relate to the processing of personal data as ancillary activities." Core activities include activities where processing of data forms is "inextricably part" of the controller's or processor's activity. Examples of such activities include hospitals and patients' health care records and private security companies and electronic surveillance of public and private spaces.

The GDPR does not define what constitutes "large scale." Recital 91 does state, however, "large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supernational level and which could affect a large number of data subjects and which are likely to result in a high risk" would be included, whereas the processing of "personal data from patients or clients by an individual physician" would not be included. The GDPR itself provides no guidance for processing activities that take place between these two extremes.

The WP29 provides some guidance, and recommends that the following factors should be considered when determining whether processing is carried out on a "large scale":

- the number of individuals concerned, as a specified number or a proportion of the relevant population;
- the volume of data or range of different data items being processed;
- the duration of the processing activity; and
- the geographical extent of the processing activity.

An example of large-scale processing provided by the WP29 is the processing of customer data in the regular course of business by a bank or insurance company.

[4] *See* Article 29 Data Protection Working Party *Guidelines on Data Protection Officers ('DPOs')* (Rev. April 5, 2017).

In the WP 29's view "Regular and systematic" activities include activities that are ongoing and occurring at particular intervals for a particular period, recurring or repeated at fixed times, occurring according to a system, pre-arranged and methodical, or carried out as part of a strategy. Examples of regular and systematic monitoring include email retargeting and data-driven marketing activities.

What Are The Key Features of the DPO's Role?

GDPR sets out specific functions and features of the DPO.

- The controller and processor must involve the DPO in all issues that relate to the protection of personal data
- The controller and processor must provide the DPO the resources she needs to perform her functions and to maintain her expertise
- The controller and processor must ensure that the DPO can work independently. The DPO cannot receive instructions from anyone, cannot be dismissed or penalized for performing her tasks, and must report directly "to the highest management level" of the controller or processor
- The DPO can be contacted by data subjects
- The DPO must be bound by confidentiality obligations

The DPO has five primary functions:

- To advise the controller or processor of its obligations under GDPR
- To monitor the controller's or processor's compliance with GDPR
- To advise regarding and to monitor the performance of any Data Protection Impact Assessment
- To cooperate with the relevant supervisory authority
- To act as the contact point for the supervisory authority

"Onward" Transfers

Underlying much of the political environment that led to the adoption of GDPR was a deep suspicion of American surveillance of personal data related to EU citizens following the Snowden revelations. This is reflected in GDPR's enactment of a specific process for the transfer of personal data to recipients outside of the EU that is intended to extend the GDPR's protections to that data even when it resides with a third party in a foreign country. In general terms, absent the explicit and informed consent of the data subject, the "onward" transfer of data to certain countries whose internal laws the EU deems not to provide "adequate" protection, like the United States, is simply prohibited unless the controller or processor transferring the data complies with this process.

Although a detailed exploration of these rules is beyond the scope of this paper, this paper provides a summary. Transfers to recipients within the US are permitted where:

- The transferor and the transferee are parties to "binding corporate rules" that provide sufficient protection. These rules would bind parties in a "group of undertakings" (perhaps an example would be two corporate affiliates owned by a common parent). They must provide a number of specific protections, they must be legally binding, and they must be approved *in advance* by the relevant supervisory authority
- The transferor and the transferee adhere to a code of conduct that has been approved by the relevant supervisory authority, or by the European Commission, in advance, and the transferor and transferee are parties to a binding agreement to adhere to that code of conduct
- The transferor and the transferee are parties to a contract including "standard data protection clauses" adopted by the European Commission. As of the date of this writing, the European Commission has not yet adopted such standard data protection clauses,[5] but it did adopt "model" data protection clauses under an earlier privacy regulation
- The transfer is pursuant to "an approved certification mechanism." In the United States, this mechanism is Privacy Shield, administered by the Department of Commerce. Transfers to recipients certified under Privacy Shield are generally permitted, although Privacy Shield is under considerable political pressure in Europe, where privacy advocates insist it fails to provide adequate protections.
- Transfers could also be permitted where the transferor and the transferee are parties to a contract containing clauses approved by the relevant supervisory authority.

Some exceptions exist:

- As mentioned earlier, where the data subject consents after having been informed of the possible risks due to the absence of an adequacy decision by the European Commission and due to the absence of appropriate safeguards
- Where the transfer is necessary to perform a contract between the data subject and the controller, or to take pre-contractual steps at the data subject's request

---

[5] The Danish supervisory authority adopted standard contractual clauses specific to GDPR in January 2020. At least one other supervisory authority has expressly approved the use of the earlier model clauses until it develops standard contractual clauses specific to GDPR. *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

- Where the transfer is necessary to perform or make a contract between the controller and a third party, if the contract is made "in the interest of the data subject"
- Where the transfer is necessary for "important reasons of public interest"
- Where the transfer is necessary for the establishment, exercise or defense of legal claims
- Where the transfer is necessary for the "vital interests" of the data subject or other persons and the data subject is physically or legally incapable of consent
- Where the transfer is from a public register satisfying specific requirements

Damages And Penalties

GDPR provides data subjects with a right to sue and to recover damages for breaches. It also empowers supervisory authorities in member states to enforce compliance through various mechanisms, including orders to cease processing. Finally, GDPR permits supervisory authorities to impose fines, which may be substantial or even crippling. For certain types of violations, these fines can be as high as the greater of €20 million or 4% of "global annual turnover." Fines of this nature are available for violations of any of the basic principles of processing, including failing to comply with the conditions of consent; for failure to honor data subjects' rights; for improper transfers to recipients in a third country; or for failure to comply with certain types of orders from supervisory authorities.

Conclusion

Compliance with GDPR requires a deep and detailed understanding of the personal data an entity actually holds. No entity can be certain it complies with GDPR if it does not know what personal data it possesses, where it got it, what it does with it, who has access to it, whether it is transferred to any third party (and if so, why, and what that third party does with it), how long the entity keeps it, and whether all of these things are consistent with what the entity has told data subjects it does with it. Performing a data inventory (or creating a data map) is usually a prudent first step. In some cases, that may be a simple process. In others, it may be a time consuming and complex undertaking that requires the help of a third party. Fortunately, it can serve dual purposes: not only is it needed to ensure that personal data is being treated lawfully, it also can serve as a key component of the record-keeping obligations imposed by the Regulation.

Compliance with GDPR is not an "event;" a business cannot simply conclude that it has achieved compliance and check that box off an in-house lawyer's or compliance manager's to-do list. Instead, compliance

is an on-going process that requires consistent monitoring to ensure that actual practices remain compliant, and to ensure that new practices also comply. Prudent entities will audit their processing activities, including regularly revisiting their vendor agreements and relationships. While this is important generally, it is particularly so when businesses acquire new entities, launch new products, or enter new business lines.

At the same time, for many businesses developing a GDPR-compliant program will be an expensive undertaking. While the risks of crippling fines—which could amount to a corporate death sentence for many businesses—is very real, US-based businesses, particularly those with no physical presence within the EU, should consider carefully, with the advice of counsel, whether GDPR actually applies to their activities.

About the Author:

MARCEL DUHAMEL

216.479.6112

mcduhamel@vorys.com

Marcel Duhamel is a partner in the Vorys Cleveland office and a member of the litigation group. He focuses his practice on privacy, consumer protection, complex litigation, class actions, electronic discovery and appellate practice. Marcel also counsels clients with respect to privacy practices and allegations of data breach. He has defended class and individual actions raising data privacy, consumer protection, FCRA, TCPA and FDCPA claims. He has advised clients with respect to GDPR compliance, financial privacy compliance, and privacy policies and has counseled clients through the Privacy Shield certification process. He is a member of the International Association of Privacy Professionals and a Certified Information Privacy Professional (CIPP/US), a Certified Information Privacy Manager (CIPM), and a Fellow of Information Privacy (FIP).


VORYS
Personal data
GDPR
EU
Protection
ivacy
Regulation
Analysis