# G.D.P.R. IS IMMINENT – IS YOUR U.S. BUSINESS PREPARED?

**Authors**
Fanny Karaman
Beate Erwin

**Tags**
Data Protection
E.U.

In Europe, an individual's right to the protection of his or her personal data is a fundamental right.[1] The E.U. General Data Protection Regulation ("G.D.P.R."), which takes effect on May 25, 2018, is aimed at protecting that right.[2]

The G.D.P.R. is notable because it applies to all companies processing personal data of persons residing in the European Economic Area ("E.E.A.") (comprising E.U. Member States as well as Iceland, Liechtenstein, and Norway) regardless of the company's location and irrespective of whether the company has a physical presence in these countries.[3]

Since the G.D.P.R. was promulgated in the form of a "Regulation," and not a "Directive," it automatically becomes law in each E.U. Member State, without the need to pass transposing domestic legislation.[4]

The G.D.P.R. replaces Directive 95/46/EC, a 1995 Directive that, until now, constituted the European framework for personal data protection. Directive 95/46/EC did so mainly by placing a compliance burden on "Controllers" of personal data (*i.e.*, legal persons requesting data processing services).[5]

Adding to the 1995 Directive, the G.D.P.R. also places a compliance burden on "Processors" (*i.e.*, legal persons providing services to the Controllers). Its purpose is to increase E.U. citizens' control over their own data by, *inter alia*, providing for more transparency, stronger data security, and protection requirements on Controllers and Processors. G.D.P.R. also implements a mechanism that can result in penalties equal to the greater of €20 million or 4% of annual worldwide turnover.[6]

---

1 Article 8(1) of the Charter of Fundamental Rights of the European Union; Article 16(1) of the Treaty on the Functioning of the European Union.

2 Chapter 1, Article 1(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 Note that under Article 7(a) of the Main Part of the E.E.A. Agreement, all E.E.A. States are obliged to adopt the G.D.P.R. Hence, the G.D.P.R. also applies to E.F.T.A. Member States Iceland, Liechtenstein, and Norway. (While a member of the E.F.T.A., Switzerland did not join the E.E.A.)

4 This does, however, not apply to E.E.A. countries, where the procedure for incorporation into domestic law consists of five phases governed by Article 102 (1) to (6) of the E.E.A. Agreement in conjunction with Regulation (EC) No 2894/94 concerning arrangements for implementing the agreement in the E.E.A.

5 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 procession of personal data and on the free movement of such data.

6 Article 83 of the G.D.P.R.; Clause 37 to the Preamble to the G.D.P.R.

During an address in New York on March 28, Mrs. Isabelle Falque-Pierrotin, president of the French Data Protection Authority (the *CNIL*), stated that the G.D.P.R. constitutes a "legal framework for trust." She explained that data protection is no longer only a legal issue. It has now also become an operational issue and must thus be viewed in an interdisciplinary way.

Translated into plain English, it means that a U.S. company like Tumblr, which is owned by Oath, a subsidiary of Verizon Communications, and targets E.U. customers, may be liable to a penalty of 4% of Verizon Communications' worldwide turnover (notably not its taxable income) for violating the G.D.P.R. This monetary penality is also accompanied by damage to the company's reputation. U.S.-owned apps that are available to E.U. customers are similarly caught by the G.D.P.R. On a smaller scale, any U.S. business with an email list that includes European customers is affected by the G.D.P.R. As a result, E.U. Member State regulators are afforded the power to prosecute a breach of the G.D.P.R. beyond the borders of the E.U.

In order to achieve clarity, the balance of this article is written in question and answer format, laying out the fundamentals of the G.D.P.R. and its impact on U.S. businesses.

## RIGHTS PROTECTED BY THE G.D.P.R.

**Q1: What rights are protected by the G.D.P.R.?**

The Regulation protects individuals located in the E.U. ("Data Subjects") with regard to the protection of their personal data.[7] It provides rules for the processing and the free movement of personal data.

Under the G.D.P.R., processing of personal data must comply with all **six general data quality principles**. In particular, personal data must be

- processed fairly and lawfully;
- collected for specific, explicit, and legitimate purposes (and not processed in a manner incompatible with those purposes);
- adequate, relevant, and not excessive;
- accurate and, where necessary, up to date;
- kept in an identifiable form for no longer than necessary; and
- kept secure.[8]

**Q2: What is personal data?**

Personal data is any information relating to the identification of an individual. More precisely it is information relating to (i) identified individuals and (ii) identifiable individuals, where "identifiable" means that an individual can be directly or indirectly identified.[9] Relevant identifiers are an individual's name, identification number, loca-

---

7 Article 1 of the G.D.P.R.

8 Article 5(1) of the G.D.P.R.

9 Article 4(1) of the G.D.P.R.

tion data, or online identifier. Also included are factors such as physical, physiological, genetic, mental, economic, cultural, or social identities of an individual.

**Q3: What is the processing of personal data?**

The processing of personal data means an operation or several operations on personal data.[10] It includes collecting, recording, organizing, structuring, storing, adaptating or altering, retrieving, consulting, using, disclosing by transmission, disseminating, otherwise making available, aligning or combining, restricting, erasing, or destroying. It is irrelevant whether such processing takes place by automated means or not. Accordingly, the G.D.P.R. applies to personal data irrespective of whether it is processed electronically or as part of a paper filing system.

**Q4: Are there different types of personal data?**

Yes. In addition to the general definition provided under Q3, certain more sensitive types of personal data are identified by the G.D.P.R.[11] Such sensitive data are subject to more stringent protection requirements. Among this sensitive data are

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union memberships,
- genetic data,
- biometric data,
- data concerning health, or
- data concerning an individual's sex life or sexual orientation.

## PERSONAL SCOPE OF THE G.D.P.R.

**Q5: Who does the G.D.P.R. apply to?**

The G.D.P.R. applies to certain Controllers and Processors.

**Q6: What is a Controller?**

A Controller is essentially the legal person that asks for the data collection. It is the legal person determining the purpose and the means of processing personal data.[12]

**Q7: What is a Processor?**

A Processor is the legal person who processes personal data on behalf of the Controller.[13]

---

10 Article 4(2) of the G.D.P.R.

11 Article 9 of the G.D.P.R.

12 Article 4(7) of the G.D.P.R.

13 Article 4(8) of the G.D.P.R.

**Q8: What are examples of a Controller and a Processor?**

The European Commission's website provides the following example:

> A brewery has many employees. It signs a contract with a payroll company to pay the wages. The brewery tells the payroll company when the wages should be paid, when an employee leaves or has a pay rise, and provides all other details for the salary slip and payment. The payroll company provides the IT system and stores the employees' data. The brewery is the data controller and the payroll company is the data processor.[14]

*"Processors and Controllers not established in the E.U. must generally designate a representative in the E.U. in writing."*

Further, the Article 29 Working Party provides the following examples:

> Example No. 2: Mail marketing
>
> Company ABC enters into contracts with different organisations to carry out its mail marketing campaigns and to run its payroll. It gives clear instructions (what marketing material to send out and to whom, and who to pay, what amounts, by what date etc). Even though the organisations have some discretion (including what software to use) their tasks are pretty clearly and tightly defined and though the mailing house may offer advice (*e.g.* advising against sending mailings in August) they are clearly bound to act as ABC instructs. Moreover, only one entity, the Company ABC, is entitled to use the data which are processed – all the other entities have to rely on the legal basis of Company ABC if their legal ability to process the data is questioned. In this case it is clear that the company ABC is the data controller and each of the separate organisations can be considered as a processor regarding the specific processing of data carried out on its behalf.
>
> Example No. 3: Company referred to as data processor but acting as controller
>
> Company MarketinZ provides services of promotional advertisement and direct marketing to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for the purpose of promoting products of other customers. This decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this processing operation.[15]

**Q9: Are all Controllers and Processors subject to the G.D.P.R.?**

No. The G.D.P.R. applies to Processors and Controllers that process data and that have an establishment in the E.U., regardless of whether their processing of

---

[14] European Commission, "What is a Data Controller or a Data Processor?"

[15] Opinion 1/2010 on the Concepts of "Controller" and "Processor" (WP 169).

personal data takes place in the E.U. or not.[16] The G.D.P.R. also applies to Processors and Controllers that are not established in the E.U. but that process personal data of individuals located in the E.U., when such processing is related to the following:

- Offering goods or services, free of charge or not, to individuals located in the E.U.
- Monitoring behavior of individuals located in the E.U., if such behavior takes place in the E.U.

Processors and Controllers not established in the E.U. must generally designate a representative in the E.U. in writing.[17] Further, Controllers can only use Processors that are in compliance with the G.D.P.R.[18]

## PROTECTION MECHANISM

**Q10: Under what circumstances can personal data be lawfully collected and processed under the G.D.P.R.?**

Personal data can generally be collected when processing is necessary for one of five reasons:

- The performance of a **contract** to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract
- Compliance with a **legal obligation** to which the Controller is subject
- Protection of **vital interests** of the Data Subject or of another natural person
- The performance of a **task** carried out in the **public interest** or in the exercise of official authority vested in the Controller
- The purposes of the **legitimate interests** pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject that require protection of personal data, in particular where the Data Subject is a child

When none of these reasons exist, personal data can generally be collected only based on **consent**.[19] Note that consent can be withdrawn at any time.[20]

**Q11: Do Data Subjects have any legal remedies under the G.D.P.R.?**

Yes. Data Subjects whose personal data has been processed in violation of the G.D.P.R. can file a complaint with the appropriate Member State's authority in

---

16 Article 3 of the G.D.P.R.

17 Article 27(1) of the G.D.P.R.

18 Article 28(1) of the G.D.P.R. For Processors that have less than 250 employees, certain record keeping requirements are waived (Article 30.5 of the G.D.P.R.).

19 Article 6 of the G.D.P.R.

20 Article 7(3) of the G.D.P.R.

charge of supervising the application of the G.D.P.R.[21] Further, Data Subjects can also bring legal action against Controllers or Processors that violate their rights under the G.D.P.R.[22]

**Q12: Do Data Subjects have the right to have their personal data deleted?**

Yes. Often referred to as "the right to be forgotten," Article 17(1) of the G.D.P.R. provides that a Data Subject has the right to obtain deletion of his or her personal data in one of the following circumstances:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
- The Data Subject withdraws consent on which the processing is based, and there is no other legal ground for the processing.
- The Data Subject objects to the processing on grounds relating to his or her particular situation pursuant to Article 21(1) of the G.D.P.R. and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of his or her personal data for direct marketing purposes, pursuant to Article 21(2) of the G.D.P.R.
- The personal data has been unlawfully processed.
- The personal data must be erased to comply with a legal obligation under E.U. or Member State law to which the Controller is subject.
- The personal data has been collected in relation to the offer of information society services directly to a child, as referred to in Article 8(1) of the G.D.P.R.

The data must be deleted "without undue delay." Currently, no definition of "undue delay" exists for this purpose. Further, the Controller must inform Processors within a "reasonable time" that the Data Subject has requested the erasure of his or her personal data. Again, no definition of "reasonable time" currently exists for this purpose.

**Q13: Can the right to be forgotten be refused?**

Yes. If processing of the personal data is necessary for one of the following reasons, the right to be forgotten does not apply:[23]

- Exercising the right to **freedom of expression and information**
- Compliance with a **legal obligation** that requires processing under E.U. or Member State law to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller
- Certain reasons of **public interest** in the area of public health[24]

---

21 Article 77 of the G.D.P.R.

22 Article 79 of the G.D.P.R.

23 Article 17(3) of the G.D.P.R.

24 See points (h) and (i) of Article 9(2) and Article 9(3).

- **Archiving purposes** in the public interest, for scientific or historical research purposes, or for statistical purposes[25] in so far as the right to be forgotten is likely to render impossible or seriously impair the achievement of the objectives of that processing
- The establishment, exercise, or defence of **legal claims**

## TERRITORIAL SCOPE AND U.S. REACH OF THE G.D.P.R.

**Q14: Can personal data be transferred to the U.S.?**

As a general rule, personal data can only be transferred outside the E.U. if the Controller and Processor are otherwise in compliance with the G.D.P.R. and one of the following requirements is met:[26]

- The European Commission has decided that (i) the third country, (ii) a territory in such country, (iii) one or more specified sectors within such country, or (iv) the international organization to which the data is to be transferred, ensures an adequate level of protection.[27]

  Note that the U.S. has not been deemed as meeting an adequate level of protection.

- Data Subjects have enforceable rights and legal remedies, and the Controller or Processor provides appropriate safeguards.

  No specific authorization from a supervisory authority is required if one of the following safeguards exist:

  - A legally binding and enforceable instrument between public authorities or bodies
  - Binding corporate rules in accordance with Article 47
  - Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)
  - Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2)
  - An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the Controller or Processor in the third country to apply the appropriate safeguards, including as regards Data Subjects' rights
  - An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the Controller or

[25] See Article 89(1) of the G.D.P.R.

[26] Article 44 of the G.D.P.R.

[27] Article 45 of the G.D.P.R.

Processor in the third country to apply the appropriate safeguards, including as regards Data Subjects' rights

Here, a specific authorisation from a supervisory authority is required:

- Contractual clauses between the Controller or Processor and the Controller, Processor or the recipient of the personal data in the third country or international organization
- Provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective Data Subject rights

If any of the above requirements are met, the transfer of personal data to the U.S. is allowed. In addition to the G.D.P.R., U.S. companies can also transfer personal data to the U.S. under the new E.U.-U.S. Privacy Shield adopted in 2016, provided they are within its scope.

***"U.S. companies with European operations or European customers should ensure adequate processes with respect to storage and processing of data under the G.D.P.R."***

## CONCLUSION

While the G.D.P.R. targets all entities collecting personal data from E.U. individuals, it has particular impact on all U.S. companies with an E.U. customer base, including tech companies. Given the significance of the penalties, compliance is essential and advisors in the cross-border field should familiarize themselves with G.D.P.R.

If actions have not already been taken, the immediate steps would be for affected U.S. companies to reach out to their existing E.U. customer base, take action to comply with the requirements of the G.D.P.R. in their communications, and request consent to the processing of their personal data by May 25, 2018. Moreover, internal processes for data security and protection should be implemented. Amongst others, these would comprise

- appointing a data protection steering committee;
- assigning a data protection officer, if required;
- performing data discovery checks with respect to data storage (identifying what, where, and how data is stored);
- performing a risk and gap analysis; and
- obtaining a legal opinion on obligations to assess exposure under the G.D.P.R.

In any event, U.S. companies with European operations or European customers should ensure adequate processes with respect to storage and processing of data under the G.D.P.R. With the May 25, 2018 deadline approaching, immediate attention to this matter is of the essence.