# The Test: Does the European General Data Protection Regulation Apply to Your Business Operating in the USA?

**BY: William Mark Mullineaux, Esq.***
**Sagan Medvec***

On May 25th, 2018, the European Union's ("EU") General Data Protection Regulation ("GDPR") goes into effect and it may shift the way you collect data, manage user information, and market to prospects even if you are not intentionally marketing to people in Europe. Despite the fact that the GDPR is complex, the use of the following test will determine whether the GDPR applies to a particular company.

**The GDPR regulates entities meeting one or both of these two criteria:**

**(1) Companies "established" in the EU and involved with processing personal data; and/or,**

**(2) Companies (a) involved with processing personal data of natural persons in the EU *and* (b) offering goods and services to natural persons in the EU *or* monitoring their behavior in the EU.**

GDPR Art. 2 ¶ 1; GDPR Art. 3 ¶ 1, 2.

"Companies" refer to all types of business entities. [1]. The full GDPR, in a well-organized format is at **https://gdpr-info.eu/art-1-gdpr/.** All of the European Union's member countries are listed in Footnote #2. [2].

The use of the test requires knowledge of the meanings of "processing," "personal data," "established," "offer goods and services in the EU," and "monitoring behavior of natural persons in the EU" and other information from the GDPR.

---

*William Mark Mullineaux, Esq. is a partner with Astor Weiss Kaplan & Mandel, LLP at mmullineaux@astorweiss.com and 215-893-4956.
*Sagan Medvec is the creative director and co-founder of BRAND LLAMA at sagan@brandllama.com and 1-877-902-7232.

This paper provides the meaning of those terms and discusses the application of the terms. This paper provides a snapshot at some of the compliance requirements but recommendations on addressing any compliance issues are beyond the scope of this article.

## I. Does the GDPR apply to Your Business?

Analysis of the answers to the following questions can be used to apply the test to any particular business.

**Question 1: Does the company or someone on the company's behalf process personal data? [Answer of "no" means GDPR does not apply]**

The GDPR only applies if there is processing of personal data. *See* GDPR Art. 2 ¶ 1. The following are the definitions of those terms.

### A. Meaning of "personal data" and "processing."

The GDPR broadly defines "*personal data*" as "any information relating to an identified or identifiable natural person…" [3]. GDPR provides that personal data includes an "online identifier" meaning that email addresses, log on information and other online information are considered personal data. [4]

The GDPR broadly defines "*processing*" as "any operation or set of operations which is performed on personal data or on sets of personal data…such as collection,…storage,… disclosure,…or destruction." [5]

Many in the United States use the term "PII" (personally identifiable information) to deal with potentially protected information. The GDPR meaning of personal data may be significantly different from a particular "PII" term in use by a company in the United States. When dealing with the GDPR, the GDPR meaning of personal data should be used and not a PII term that is familiar to the company.

If a company has or controls any personal information of a natural person and does *anything* with that information, it very likely that the company is processing personal data as defined in the GDPR. It is hard to imagine a business activity of a significant size that does not involve processing of personal data as defined by the GDPR.

Some common examples of personal data processing would include collecting email addresses for email newsletter or completing the contact form on your website. Even putting information from someone's business card in your CRM or sales management tool may be included in these definitions.

**B. The GDPR applies to "Controllers" and "Processors."**

For the GPDR to apply, a company must be a "Controller" or a "Processor" as defined by the GDPR.

A "controller" means a "natural or legal person…which, alone or jointly with others, determines the purposes and means of the processing of personal data…." GDPR Art. 4 ¶ 7 [6]. "Processor" means "a natural or legal person which processes personal data on behalf of the controller." GDPR Art. 7 ¶ 8 [7]. The controller, alone or with others, is the "brains" and the processor does the processing on behalf of the controller.

A controller has responsibility for the work of the processor since the processor is acting *on behalf of* the controller. A controller also has responsibility when it acts jointly with others when determining the purposes and means of the processing of personal data.

If a company is not a "Controller" or a "Processor" as defined by the GDPR the GDPR does not apply. For example, a business owner who has a website that collects information in a contact form would be considered a "Controller." An email marketing tool like Constant Contact or your website design firm that created the website may be considered a "Processor."

**Question 2: Does a Company have processing activities related to (a*) offering of goods or services* to natural persons in the EU *or* (b) *monitoring their behavior* in the EU? [Answer of "yes" means GDPR applies]**

The GDPR regulates Controllers and Processors ***not*** established in the EU if processing activities relate to (a*) offering of goods or services* to natural persons in the EU or (b) *monitoring their behavior* in the EU.

Article 3.2 (Territorial Scope) of the GDPR in part provides:

> (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 behaviour as far as their behaviour takes place within the Union.

GDPR Art. 3 ¶ 2 (emphasis added)

GDPR Article 3 is very clear that the GDPR will regulate United States companies ***not*** established in the EU if the company does processing of personal data related to offering goods or services in the EU ***or*** monitoring behavior in the EU.

This raises the question of the type of activities actually needed to satisfy the requirement of "processing related to the offering of goods or services." GDPR Art. 3 ¶ 2(a). Recital 23 provides the following factors to be considered on the issue:

> factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union.

GDPR, Rec. 23

The factors in Recital 23 indicate that just having a website accessible worldwide would not subject a company to regulation by the GDPR. A company would have to go further, like using the language or currency of any particular EU country or mentioning customers or users in

the EU. On the other hand, if a company actually makes a sale or provide services in the EU, that would appear to be an affirmative activity that would generate jurisdiction over that company.

Article 3 also raises the question of the activity needed to satisfy the requirement of "the monitoring of their behaviour … within the Union." GDPR Art. 3 ¶ 2(a). The requirement for monitoring is met, for example, if "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes." GDPR Rec. 24. In other words, the monitoring element is met if data is used to profile a natural person to predict preferences, behaviors and attitudes.

**Question 3: Is the company processing personal data and *"Established"* in the EU as defined by the GDPR? [Answer of "yes" means GDPR applies]**

> Article 3.1 (Territorial Scope) of the GDPR in part 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.

GDPR Art. 3 ¶ 1 (emphasis added)

The GDPR regulates Controllers and Processors that process personal data and that are "established" in the EU regardless of whether the processing takes place in EU. As discussed above, it is very likely that a company of any size does process personal data, making that element easy to establish. The question becomes whether a company is "established" in the EU. A company is "established" if it has "effective and real exercise of any stable arrangements" in the EU. *See* Recital 22 of GDPR [8]. That means that a company must have more than a fly-by-night presence in order for the GDPR to apply to the company. Unfortunately, the term

"effective and real exercise of any stable arrangements" in the EU is the type of term over which there is uncertainty and litigation.

As an example, under the GDPR, a parent company with no direct activity in the EU could be deemed to be established in the EU by activity of a subsidiary. The GDPR specifically states that "[t]he legal form of such arrangements, whether through a branch or *a subsidiary* with a legal personality, is not the determining factor in that respect." GDPR Rec. 22. (Emphasis added).

For the GDPR to apply pursuant to Article 3.1, it is *not* required that the company process personal data from an individual *in the EU.* Under the literal meaning of Article 3.1, if a parent processes personal data from *only outside the EU*, the GDPR would still apply if the parent through a subsidiary is considered established in the EU. *See* GDPR Art. 3 ¶ 1. A United States Court *may* not find jurisdiction against a parent based on these facts. If a parent itself has no direct contact with the EU and did not process any personal data from the EU, there could be a significant jurisdiction issue. Of course, most companies would not want to spend the time and money it would take to convince a court that the GDPR's claim to jurisdiction goes too far and the GDPR does not have jurisdiction over that company. An analysis of international jurisdiction is beyond the scope of this paper.

**II. Exceptions: The GDPR does not apply to authorities investigating or preventing crime or to natural persons in the course of purely personal or household activity.**

The GDPR does not apply to the processing of personal data "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." GDPR Art. 2 ¶ 4.

The GDPR does not apply to the processing of personal data "by a natural person in the course of a purely personal or household activity." GDPR Art. 2 ¶ 3.

### III. It is a myth that the GDPR does not apply to companies outside of the European Union.

Companies based in the United States are subject to GDPR compliance requirements if they are involved in processing personal data of people in the EU. The scope of these requirements is significant in reach and while they may be challenged in the future, they may currently impact a business severely with extremely high fines. Additionally, if you are a company targeting the EU for business and collecting any PII you may have to register a third-party as a representative within the boundaries of the EU to respond to violations of GDPR regulations. A third-party data protection authority agency may need to be named in your privacy policy and/or terms of use of your website or app as well to support the response to violations.

### IV. The GDPR applies to companies with less than 250 employees.

There is a misconception that the GDPR does not apply to companies with fewer than 250 employees. The GDPR does apply to those smaller companies.

The GDPR gives companies with less than 250 employees "a break" because those companies have a reduced record keeping requirement. The reduced requirement, however, does not apply if the company's processing is likely to result in a risk to the rights and freedoms of natural persons from the EU, or the processing is not occasional, or the processing includes special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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) or personal data relating to criminal convictions and offences.

**V. List of some of the GDPR compliance requirements.**

Compliance requirements that apply to a particular company will depend on a variety of factors including the type and amount of data used by a company. This paper provides a snapshot of *some* of the compliance requirements and does not give any advice on how to comply. These are some of the GDPR compliance requirements:

- Processing of EU personal data must have a lawful basis listed in Article 6 of the GDPR.
- One of the six lawful grounds for processing data is *consent* of an individual. If consent is relied upon it must be given with deliberate action to opt in, not pre-ticked boxes
- Data Breach Notification Obligations
- Individual rights to information and access of data
- Individual rights to modify personal data and to have personal data erased
- Accountability regulations
- Data security regulations
- Record-keeping regulations
- Delegation of Processing- the company delegating processing must obtain written commitment from processor to comply with GDPR's obligations
- Potential fines *up to* 20 million Euros or 4% of annual revenue, whichever is greater
- Required Appointment of Data Protection Officer

  The following companies must appoint a data protection officer:

  - Public authorities or bodies, except for courts acting in their judicial capacity.
  - Companies who process data requiring regular and systematic monitoring of data subjects on a large scale.
  - Companies who process, on a large scale, any special category of personal data. This includes data which reveals racial or ethnic origin; political opinions; religious beliefs and other such information listed in Section IV above.
  - Companies who process, on a large scale, personal data relating to criminal convictions and offences

  All of these regulations can be found at **https://gdpr-info.eu/art-1-gdpr/**

**FOOTNOTES:**

[1] In this paper, "companies" refers to all types of businesses, including Sole Proprietor, Partnership, General Partnership, Limited Liability Partnership, Corporation, Nonprofit Corporation, Limited Liability Company, Joint Venture, Association and any other type of legal entity.

[2] The countries in the EU are: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. The UK plans to finish withdrawing from the EU by March 29, 2019.

[3] The GDPR definition of "personal data" is

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

GDPR Art. 4, ¶ 1. The definition is broad. Note that the inclusion of an "online identifier" applies to all persons that have electronic communications with the company and that contributes to the definition being very broad.

[4] *Id.*

[5] The GDPR definition of "processing" is

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

GDPR Art. 4, ¶ 2. The definition is broad.

[6] The GDPR definition of "controller' is:

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

GDPR Art. 4, ¶ 7.

[7] The GDPR definition of "processor' is

> a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

GDPR Art. 4, ¶ 8.

[8] Recital 22 of GDPR provides:

> Processing by an establishment. Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

**Disclaimer**

This paper is for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem. This paper does not create an attorney-client relationship with the authors.