GDPR: Fiction versus Fact

This document discusses in general terms the EU General Data Protection Regulation (GDPR) and does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

One of the main challenges for organizations is getting the resources to sort through the facts, and the fictions, of the GDPR. You may have come across contradictory information about what the GDPR requires. With that in mind, Salesforce put together this guide to help clarify some common confusions around the GDPR. For more background about the GDPR and what it does, check out the Salesforce Trailhead.

Fiction: "Processing European personal data requires the consent of the data subject."

> **Fact:** There are six available lawful bases for processing. Consent is only one of them. For instance, personal data can also be processed:
>
> - when necessary for the performance of a contract to which the data subject (the individual whose data is processed) is a party;
> - when there is a legal obligation to process the data (such as the submission of employee data to a tax authority); and
> - on the basis of legitimate interests, such as commercial and marketing goals. The legitimate interest must, however, outweigh any detriment to the privacy of the data subject.

Fiction: "European personal data must be stored within Europe."

> **Fact:** *The GDPR does not require information to be stored in Europe*. However, transfers of European personal data outside the European Economic Area (EEA) generally require that a valid transfer mechanism be in place to protect the data once it leaves the EEA (Articles 44-50). The CJEU has recently confirmed the validity of the European Commission's standard contractual clauses as a legal mechanism for the transfer of EU personal data, but invalidated the EU-US Privacy Shield framework. Salesforce's customers can use our services, relying on Salesforce's Processor Binding Corporate Rules and the European Commission's standard contractual clauses, both of which are already included in our Data Processing Addendum. Please find more information about these transfer mechanisms here.

Fiction: "The GDPR requires EU personal data to be encrypted at rest."

> **Fact:** The GDPR requires organizations to take technical and organizational security measures which are *appropriate* to the risks presented. Article 32 of the GDPR

includes encryption as an example of an appropriate technical measure, depending on the nature and risks of your processing activities. In other words, encryption at rest and pseudonymization may be appropriate depending on the circumstances, but they are not mandated in every instance.

Fiction: "EU data subjects have an absolute right to have their personal data deleted upon request."

Fact: The right to have one's data deleted is often referred to as "the right to be forgotten." However, the right to be forgotten is not an absolute right. It has a limited scope and is subject to certain limitations. In most cases, when considering a request for deletion several relevant factors should be taken into account; this right will not apply, for example, if the processing is necessary for compliance with a legal obligation.

Fiction: "A data protection officer is mandatory for all companies subject to the GDPR."

Fact: A data protection officer is required by the GDPR only when one of the following applies:

- the organization is a government institution;
- the organization processes certain sensitive types of data (such as data on health or religion) on a large scale as part of its core activities; or
- the organization systematically monitors people (for example, via cameras, or software which tracks internet behavior) as part of its core activities.

Fiction: "The GDPR requires a data protection impact assessment for all processing activities involving EU personal data."

Fact: A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. Under the GDPR, a DPIA is necessary only for processing that is likely to result in a high risk to individuals, such as the following:

- large-scale processing of certain sensitive types of EU personal data, such as data concerning a person's health;
- systematic and extensive automated decision-making which produces legal or similarly significant effects on individuals, such as the use of fraud detection software; or
- systematic and large-scale monitoring of public space (for example, with cameras).

Fiction: "Profiling and automated decision-making is prohibited under the GDPR."

Fact: Profiling of EU individuals and automated decision-making involving EU personal data are not prohibited, but these processing activities may be subject to certain conditions. In particular, when decisions which legally or similarly significantly affect an individual are made automatically, the data subject:

- must be given meaningful information about the underlying logic, and about the significance and potential consequences for them; and

- must in some cases have the ability to require that a human being is involved in the process .

A DPIA may also be required.

Fiction: "If an organization is established outside the EU, the GDPR does not apply to its processing of EU personal data."

Fact: Regardless of where an organisation is established, the GDPR applies to EU personal data which is processed in the context of:

- offering goods and services (whether paid or not) to people in the EU; or
- monitoring the behavior of people in the EU, for example by placing cookies on the devices of EU individuals (Article 3(2)).