GDPR: Fiction versus Fact

As you gear up your organization to comply with the forthcoming EU General Data Protection Regulation (GDPR), you may come across contradictory information about what the GDPR does -- and does not -- require. One of the main challenges for organizations who are facing GDPR compliance is getting the resources to sort through the facts, and the fictions, of this new law. With that in mind, Salesforce put together this guide to help clarify some common confusions around the GDPR and get you and your organization on the path towards compliance. 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:** Consent is only one of the legal bases one can use for the processing of personal data (Article 6(1)(a)). 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 do so (such as the submission of employee data to a tax authority); and
> - sometimes even 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 contain any obligation to store information 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 (Chapter V, Articles 44-50). Salesforce ensures that its customers can comply with this by offering its customers a data processing addendum (DPA) that incorporates Salesforce's processor Binding Corporate Rules, EU-U.S. and Swiss-U.S. Privacy Shield Certification, and the Model Clauses as approved by the European Commission. Please find more information about these transfer mechanisms here.

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

> **Fact:** The GDPR does not mandate specific security measures. Instead, the GDPR requires organizations to take technical and organizational security measures which are *appropriate* to the risks presented (Article 32(1)). Encryption at rest and pseudonymization may be appropriate depending on the circumstances, but they are not mandated by the GDPR 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 (Article 17). In most cases, when considering a request for deletion several relevant factors have to be taken into account; this right will not apply, for example, if the processing is necessary for compliance with a legal obligation.

However, data subjects do have an absolute right to prevent their personal data from being processed for direct marketing purposes.

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

Fact: A data protection officer is only required by the GDPR 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 their core activities; or
- the organization systematically monitors people (for example, via cameras, or software which tracks internet behavior) as part of their core activities (Article 37(1)).

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

Fact: Under the GDPR, a data protection impact assessment (DPIA) is only necessary when it concerns high-risk processing of EU personal data, 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; and
- systematic and large-scale monitoring of public space (for example, with cameras) (Article 35(3)).

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 (Article 22(3)).

A data protection impact assessment (see Myth 6 above) 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 organization 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)).