The EU General Data Protection Regulation

What will change and what it means

Trunomi revolutionises data sharing for the financial industry; connecting financial service providers to their customers over a secure customer-driven consent-based data sharing platform. Enabling customers to digitally control and share their personal data in full compliance with data privacy regulations (EU GDPR).

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016 and will be directly application in all member states from May 2018 – at which time those not complying will face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organisations across the region approach data privacy.

This report outlines the key changes to data protection laws, and explains the penalties of non-conformance.

The aim of the General Data Protection Regulation (GDPR) is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 Directive was established.

Although Directive 95/46/EC was meant to bring together the laws of different member states, it was still a directive, which left some room for interpretation during the transposition into individual national law. This fact, along with today's rapidly changing data landscape, has led to the necessity for another update to the regulatory environment of the EU. The incoming GDPR is a much larger piece of legislation, and, as a regulation and not a directive, it will become immediately enforceable law in all member states.

The main principles on privacy are still true to form with both the previous directive and the OECD guidelines; however, social media and cloud storage were not a reality in 1995 as only about 1% of the European population was using the internet. With modern technology, we are creating more personal data than ever before, and the processing of that data has become ubiquitous. The GDPR is meant to update the standards to fit today's technology while remaining general to simply protect the fundamental rights of individuals throughout future waves of innovation.

The key points of the GDPR, as well as information on the impacts it will have on business, can be found below.

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.

Previously, territorial applicability of the Directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear – it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Organisations in breach of the GDPR can be fined up to 4% of their annual global turnover or €20m (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts (see below). There is a tiered approach to fines, e.g. a company can be fined 2% for not having their records in order (Article 28), not notifying the supervising authority and data subject about a breach, or not conducting an impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Breach notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to 'result in a risk for the rights and freedoms of individuals'. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, 'without undue delay' after first becoming aware of a data breach.

Right to access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in Article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subject's rights to 'the public interest in the availability of the data' when considering such requests.

Data portability

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly used and machine readable format' and have the right to transmit that data to another controller.

Privacy by design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically: 'The controller shall... implement appropriate technical and organisational measures... in an effective way... in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices;
- may be a staff member or an external service provider;
- contact details must be provided to the relevant DPA;
- must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge;
- must report directly to the highest level of management; and
- must not carry out any other tasks that could results in a conflict of interest.

FAQs

When is the GDPR coming into effect?

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and, unlike a Directive it does not require any enabling legislation to be passed by government; meaning it will be in force by May 2018.

Who does the GDPR affect?

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What are the penalties for non-compliance?

Organisations can be fined up to 4% of annual global turnover for breaching the GDPR, or €20m. This is the maximum fine that can be imposed for the most serious infringements, such as not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

What constitutes personal data?

Any information related to a natural person or 'Data Subject', which can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

What is informed and explicit consent?

The conditions for consent have been strengthened, as companies will no longer be able to utilise long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

What is the difference between a regulation and a directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast to the previous legislation, which is a directive.

Does my business need to appoint a Data Protection Officer (DPO)?

The proposals surrounding the mandatory appointment of a DPO vary among the drafts by each EU authority. The Commission requires a DPO for any business over 250 employees, the Parliament covers entities processing the personal data of over 5,000 individuals, and the Council opinion does not make DPOs mandatory.

How does the GDPR affect policy surrounding data breaches?

Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.