


Your data

The General Data Protection
Regulation and you

Eastbourne Ordinariate Mission 

Information from eugdpr.org and Trunomi
Cover image of *Nomade* (Jaume Plensa, 2007; Des Moines) via pxhere.com



The General Data Protection Regulation (“GDPR”) is legislation which comes directly from the EU without the need to be interpreted by national parliaments. It becomes law throughout the EU on 25 May 2018. The UK Government has indicated that this law will not be affected by leaving the EU.

The aim of 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 previous directive was established in 1995. Although the key principles of data privacy still hold true to that legislation (in the UK, the Data Protection Act 1998), many changes have been proposed to the regulatory policies. This leaflet lists the key points of the GDPR for you as a “data subject” and for organisations.

Increased territorial scope

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. GDPR 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

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (around £18m), 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. 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 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 organisations 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.

Data Subject Rights

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 subjects’ 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 carry out the processing.

Data Protection Officers (“DPOs”)

Currently, controllers are required to notify their data processing activities with local Data Protection Authorities (“DPAs”) like the Information Commissioner’s Office in the UK, which can be a bureaucratic nightmare for multinationals, with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications/registrations of data processing activities to each local DPA, nor will it be a requirement to notify/obtain approval for some transfers. Instead, there will be internal record keeping requirements, and appointing a DPO 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 (including religious affiliation) or data relating to criminal convictions and offences.

Importantly, the DPO:

- ▶ must have suitable professional qualities and, in particular, expert knowledge on data protection law and practices
- ▶ may be a staff member or an external service provider
- ▶ must provide contact details 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
- ▶ must not carry out any other tasks that could result in a conflict of interest.