[**Preparing for the General Data Protection Regulation –**](https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf) **GDPR (2018)**

Enforcement date: **25th May 2018** - at which time those organizations in non-compliance may face heavy fines.

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

***GDPR Key Changes***

​The aim of the 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 the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; 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**

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (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 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.​

***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 subjects 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. The GDPR requirements will force companies to change the way they process, store, and protect customers’ personal data. For example, companies will be allowed to store and process personal data only when the individual consents and for “no longer than is necessary for the purposes for which the personal data are processed.” Personal data must also be portable from one company to another, and companies must erase personal data upon request.

**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 use 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 it.

**Data Protection Officers (DPO)**

Currently, controllers are required to notify their data processing activities with local DPAs. 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 if there are more than 250 employees. Importantly, the DPO:

* Must be appointed on the basis of professional qualities and, in particular, 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 not carry out any other tasks that could results in a conflict of interest.​
* Inform and advise the organisation of its obligations.
* Monitor compliance, including awareness raising, staff training and audits.
* Cooperate with data protection authorities and act as a contact point.



<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>

***What types of privacy data does the GDPR protect?***

* Basic identity information such as name, address and ID numbers
* Web data such as location, IP address, cookie data and RFID tags
* Mobile Phone Devices
* Health and genetic data
* Biometric data
* Racial or ethnic data
* Political opinions
* Sexual orientation

***Steps to prepare for the GDPR?***

**Conduct a Risk assessment:**

You want to know what data you store and process on EU citizens and understand the risks around it. Remember, the risk assessment must also outline measures taken to mitigate that risk. A key element of this assessment will be to uncover all shadow IT that might be collecting and storing PII. Shadow IT and smaller point solutions represent the greatest risk for non-compliance; ignore them at your own peril.

**Hire or appoint a DPO:**

If the organisation has more than 250 employees. The GDPR does not say whether the DPO needs to be a discrete position, so presumably a company may name someone who already has a similar role to the position as long as that person can ensure the protection of PII with no conflict of interest. Otherwise, you will need to hire a DPO. Depending on the organization, that DPO might not need to be full-time. In that case, a virtual DPO is an option. GDPR rules allow a DPO to work for multiple organizations, so a virtual DPO would be like a consultant who works as needed.

**Create or Update Data Protection Plan:**

Most companies already have a plan in place thus they will simply need to review and update it to ensure that it aligns with GDPR requirements.

**Create a plan to report your GDPR compliance progress:**

Organizations must demonstrate that they are making progress against completing the Record of Processing Activities (RoPA)—article 30 of the GDPR regulation which is centred around taking inventory of risky applications—to avoid being an easy target for regulators. Establishing the RoPA, is the essential piece to focus on at this stage in the game as it enables organizations to identify where personal data is being processed, who is processing it and how it is being processed.