GDPR factsheet

The General Data Protection Regulation (GDPR) is the pan-European privacy law. From 25 May 2018, all organisations that process personal data of EU citizens must comply with this strict new law. So, what has changed? And what do you need to change?

1. Your activities are much more likely to be covered by EU privacy legislation

If your organisation processes personal data of individuals residing in the EU, you must comply with the GDPR. It does not matter whether or not your organisation is established in the EU or if the processing takes place within the EU or not. And if there was any doubt before: the definition of personal data now explicitly includes online identifiers, such as IP addresses or cookie IDs.

2. Some of the legal grounds for processing personal data become more stringent

As with current privacy legislation, the GDPR prescribes that there must be a legal basis for all processing of personal data. Consent provides such a legal basis. Although the legal bases have remained the same, obtaining consent under the GDPR may become significantly harder. The GDPR now clearly states that consent must be given by a statement or a clear affirmative action. Silence, pre-ticked boxes and inactivity do not constitute consent. Other legal bases for the processing of personal data are:

- processing which is necessary for the performance of a contract;
- compliance with legal obligations*;
- protecting the vital interests of individuals;
- the fulfilment of a public interest; and
- a legitimate interest pursued by the controller or a third party, which is not disproportionate to the interest of the individual(s) whom it concerns.

*However, legal obligations are now explicitly narrowed down to compliance with EU law or the laws of a Member State. Consequently, organisations that are subject to non-EU legislation may face challenges in this respect.

3. Your privacy statement must be even more transparent

You must explain clearly and fully, using plain language, how and why you use personal data. Furthermore, you must inform individuals of their enhanced rights, such as the right to view their data, to amend or erase the data if there are clear mistakes, to object to processing, and to transmit their data to another service provider (*right to data portability*). If you create profiles based on individuals' data, you must destroy them upon their request. Finally, you should remember to explicitly mention the right to file a complaint with the supervisory authority.

4. You may need to enable ‘data portability’

If you offer an online service that allows people to store their personal information, they must be able to transmit all their information in structured, commonly used and machine-readable format to another organisation. For instance, this might involve downloading photos, social media posts or forum contributions. This right does, however, not apply where the processing of personal data is based on a legal ground other than consent or a contract, such as the processing of personal data necessary for compliance with a statutory obligation.

5. You must also publish an internal privacy policy

You need to document how personal data is handled and secured within your organisation. Raising awareness of this policy among employees is key. Periodic training will also be required.

6. You must keep records of all personal data processing activities

These records must include, among other things, a description of the personal data being processed, the purposes for which they are processed, and how they are secured. This obligation applies to organisations with more than 250 employees, but also to organisations with fewer than 250 employees if they process personal data on a regular basis or they process special categories of personal data (e.g. biometric data or data concerning an individual's health).

7. You must document all data breaches internally

Under current privacy legislation, you are required to document only those data breaches that you are obliged to report to the supervisory authority. The GDPR makes it compulsory to document *all* data breaches internally, even those which you are not required to report. If you process personal data on someone else's behalf (a 'controller'), the GDPR also imposes a legal obligation to report all data breaches that occur during such activities to the controller, so that the controller can notify the supervisory authority.

8. You need to know where your personal data is stored, and may need extra safeguards

If you store personal data with a third party in another country, you must check whether the data is stored within or outside the EU. The latter is only permitted if the third party meets strict legal requirements, for instance when the country in question has been certified by the European Commission. With regard to third parties in the United States, the so-called Privacy Shield offers the necessary safeguards. However, please note that customers may demand that their data simply does not leave the EU at all.

9. Your data processing agreements with suppliers and customers must be revised

The GDPR contains more specific requirements for data processing agreements, which must be concluded if you process personal data on behalf of another organisation (a 'controller'), or if

another organisation (a 'processor') processes personal data on your behalf. For example, if you process personal data on behalf of a controller, you need permission before subcontracting any of your processing activities.

10. You must carry out a thorough Privacy Impact Assessment (PIA) for activities posing a high risk

A PIA is an extensive assessment intended to identify privacy risks, and to eliminate such risks as much as possible, so that the privacy of individuals is not put in jeopardy beyond what is strictly necessary and proportionate. You may not carry out a processing activity which poses a risk to privacy until after the PIA has been conducted and its outcomes have been implemented.

11. 'Privacy by design' and 'privacy by default'

This means that privacy considerations must be identified and incorporated at every step in the development process. This can be achieved by using techniques such as pseudonymisation and by processing as little personal data as possible, e.g. by processing only the necessary personal data. This requirement of necessity also applies to the accessibility of data (i.e. who has access to which data) and the period for which data is stored. The default settings of a product or service must also be as privacy-friendly as possible. Products and services will therefore have to be developed and designed in such a way as to safeguard that they are 'privacy proof'.

12. Your security measures must be fit for purpose, both now and in the future

The security of personal data is of paramount importance. If you don't restrict access to only those users with a need-to-know, using strong (multi-factor) authentication and encryption, if you don't use TLS, firewalls, anti-virus software, or if you don't patch your software and systems in time, you are at serious risk. You are also at risk if the security measures are not regularly evaluated and updated.

13. You may need to appoint a Data Protection Officer (DPO)

A data protection officer is an independent person advising and reporting on GDPR compliance. Appointing a DPO is compulsory if you are a public body, if you process sensitive personal data (such as medical records) on a large scale, or if you are engaged in regular and systemic monitoring of people's activities on a large scale. The DPO can be appointed either internally or externally.

14. You may need to pay special attention to biometric data

Does your organisation make use of fingerprints or other biometrics, e.g. for access control? Then you need to comply with the GDPR's strict protection regime for biometric data.

15. Fines under the GDPR are drastically higher

Under the GDPR, the supervisory authorities may issue penalties of up to EUR 20 million or 4% of the annual worldwide turnover, whichever is higher. Furthermore, not complying with the GDPR may have a severe impact on your organisation’s reputation.