naomi korn

ASSOCIATES

Data Protection FAQs

Q. What is the GDPR?

A. The GDPR is the 'General Data Protection Regulation', which came into force on 25 May 2018 as the Data Protection Act 2018. The GDPR harmonised data protection rules across EU member states. It applies to processing carried out by individuals and organisations operating within the EU, but also applies to organisations outside the EU that offer goods and services to EU citizens. The GDPR significantly enhances the rights of data subjects in the processing of their personal data. Data Protection laws are nothing new. In the UK, we have had data protection laws since 1998 (Data Protection Act 1998). GDPR is an uplift on existing data protection laws therefore.

Q. What is a 'Regulation'?

A. A regulation is a legal act of the European Union that becomes immediately enforceable as law in all member states simultaneously. Regulations can be distinguished from directives which need to be transposed into national law.

Q. Will the GDPR apply in the UK after we have left the EU?

A. Yes. The government has taken the decision to implement the GDPR into UK law irrespective of Brexit.

Q. Do we need a Data Protection policy?

A. Yes, you will need to have a Data Protection policy in place, which describes how you comply with data protection laws. However GDPR is more than writing a policy. It means that you have an organisation wide approach to protecting the privacy of the data subjects for whom you hold and process personal data. This means that your governing body understands its obligations under data protection law and that your organisation as a whole applies the data protection principles in all your data collection and processing activities.

Q. What is personal data?

A. Personal data means data which relate to a living individual who can be identified from that data, or from that data when combined with other information in possession of a data controller or data processor. It includes any expression of opinion about an individual.

The definition of personal data has been enhanced under the GDPR. The European Commission defines personal data as:

> '*any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking website, medical information, or a computer's IP address.'*
> *http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en*

With reference to personal data and the GDPR, the ICO says:

> *'Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.*
> *For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.'*
> https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Q. What is sensitive personal data?

A. Sensitive personal data means personal data which contains information about a data subject which tells you about private aspects of his/her life such as racial origin, political opinions, health and sexual life. There is a presumption in data protection law that sensitive personal data is private, open to misuse and therefore needs to be treated with even greater care than other personal data.
Under the GDPR the definition of sensitive personal data has been expanded to include genetic and biometric data.

Q. Do all personal data breaches need to be reported to the ICO?

A. Under the current UK data protection law, most personal data breach reporting is best practice but not compulsory. Under GDPR it *will* be mandatory to report a personal data breach *if it's likely to result in a risk to people's rights and freedoms.* If it's unlikely that there's a risk to people's rights and freedoms from the breach, you don't need to report. The best approach will be to start examining the types of incidents your organisation faces and develop a sense of what constitutes a serious incident in the context of your data subjects and the data you collect. Organisations need to remember that if there's the likelihood of a *high* risk to people's rights and freedoms, they will also need to report the breach to the individuals who have been affected.
See https://iconewsblog.org.uk/2017/09/05/gdpr-setting-the-record-straight-on-data-breach-reporting/

Q. Do I have to have consent from the data subject in order to process their personal data?

A. No. Organisations must have a 'lawful basis' or 'grounds for processing' before they can legally process personal data. Consent is *one of six* grounds for processing personal data – and any processing must be justified using one of these grounds.

If you rely on consent as a justification for processing, the GDPR asks data processors to seek 'clear, affirmative action' to indicate consent from data subjects – pre-ticked opt-in boxes are not indications of valid consent. Consent must be clear and precisely explained so the data subject knows exactly how their personal data is being used. And remember that if you are using consent as grounds for processing, data subjects have increased rights to withdraw their consent.

For ICO guidance on consent see: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf)

For more about grounds for processing see https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

Q. Will we be heavily fined if we breach the GDPR?

A. The answer to this question from the ICO is:

> '*This law is not about fines. It's about putting the consumer and citizen first. We can't lose sight of that. Focusing on big fines makes for great headlines, but thinking that GDPR is about crippling financial punishment misses the point.' 'It's true we'll have the power to impose fines much bigger than the £500,000 limit the DPA allows us. It's also true that companies are fearful of the maximum £17 million or 4% of turnover allowed under the new law. But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm*.'
> https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/

Q. Do we have to employ a Data Protection Officer?

A. The GDPR requires that it is mandatory for the following types of organisation (whether data controllers or processors) to appoint a DPO:

- all public authorities and bodies (irrespective of what personal data they process)
- organisations whose core activity is monitoring individuals regularly and systematically, on a large scale or
- organisations whose core activity consists of processing on a large scale, special categories of personal data or personal data relating to criminal convictions and offences.

If your organisation is small and you don't fit the above criteria, you still have to make sure that someone in the organisation is responsible for your legal obligations, and has a reporting line directly to the governing body.

Q. How long can we keep data?
A. The DPA/GDPR don't stipulate how long personal data should/could be kept but, following the data protection principles, you can't keep data *for longer than your purposes for collecting it.* You should have identified the appropriate length of time for Keeping data in an Information Asset Audit, and communicate that length of time to the data subject in your Privacy Notice.
With some data assets you may have a reason to keep the data for longer than its original purpose, for example for archival purposes.

See: https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/ for more on grounds for consent

See https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices for examples of Privacy Notices from schools

Q. Do we have to register with the ICO if we are a data controller or processor?
A. Under the Data Protection Act some organisations were required to 'notify' (i.e register) at https://ico.org.uk/for-organisations/register/ . This register, which contains quite extensive details about an organisation's data processing, will end with the GDPR. Organisations with a Data Protection Officer will have to register their contact details with the ICO, as well as make their contact details available on their organisation's website.

Q. We use CCTV. Do we have obligations under GDPR?
A. Under current data protection laws, most organisations using CCTV have to notify the ICO.

> *' Images of people are covered by the Data Protection Act, and so is information about people which is derived from images – for example, vehicle registration numbers. Most uses of CCTV by organisations or businesses will be covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.'*
> **https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/**

Under the GDPR the rights of data subjects are significantly enhanced and if you are planning to install CCTV, or already using it, you will need to carry out a Privacy Impact Assessment and make a decision about whether CCTV is the most reasonable way for you to achieve your purposes. You may find through the PIA that your use of CCTV impacts

negatively on the rights and freedoms of the people being filmed, in which case you do not have good grounds for using CCTV.
There is a CCTV code of Practice from the ICO at https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Q. Do we have to get someone's consent to process their data on a computer?
A. Processing personal data on computer or in paper filing systems requires 'grounds for processing'; there are 6 grounds for processing, only one of which is consent. Just because you are going to store personal data on computer does not mean that you have to get the consent of the data subject.

Q. Do we need new GDPR software?
A. The software you are using needs to support you to implement data protection laws. If your software doesn't support you to, for example, delete personal data or 'pseudonymise' data, you need to talk to your software supplier to discuss how functionality might be improved. For many people buying new software is a last port of call, however, if you do decide that you need new software, ensure that you design privacy compliance into the functionality of the system.

Q. What about the personal data of children under 16?
A. EU countries can make individual decisions about the age of consent for allowing the processing of personal data in online services. In the UK, the age is 13.

For further information see:

- www.ico.org.uk
- Overview of the GDPR at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/