Data Protection Act 2018

##  **Changes to Data Protection Under GDPR**

Data protection law in the UK is based on the 1998 Data Protection Act. However, with continued changes in technology In May 2018, the **General Data Protection Regulation (GDPR)** replaced the Data Protection Act and imposed many new responsibilities and sanctions on organisations.  The eight principles of data protection laid out in the 1998 Data Protection Act will remain relevant, with changes to some of the key principles. Below is an overview of the eight principles of data protection, with guidance on the changes and what they could mean for your business.

**The new and amended UK Data Protection Act**

Now that Brexit has happened, several legal changes has taken effect in the area of data protection.An**[interim period of six months](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-statement-in-response-to-uk-governments-announcement-on-the-extended-period-for-personal-data-flows-that-will-allow-time-to-complete-the-adequacy-process/%22%20%5Ct%20%22_blank)** (until June 2021) has been agreed to by both the UK and EU, and ensures the free flow of data between the two blocs.

**The Data Protection Act**

The [Data Protection Act 2018](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

* used fairly, lawfully and transparently
* used for specified, explicit purposes
* used in a way that is adequate, relevant and limited to only what is necessary
* accurate and, where necessary, kept up to date
* kept for no longer than is necessary
* handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

**The Eight Principles of Data Protection**

**1. Fair and lawful**

Your organisation must have legitimate grounds for collecting the data and it must not have a negative effect on the person or be used in a way they wouldn’t expect. Organisations are required to provide full transparency about how they wish to use the data, as well as ensure their data is only used in ways customers would expect. Detailing precisely what a consumer’s information is being used for allows them to make an informed decision as to whether to share certain pieces of personal information.

**Changes under GDPR**

Under GDPR, conducting criminal record checks on employees must be justified by law. For example, a school is far more likely to be permitted to carry out such checks on their teachers than a restaurant hiring kitchen staff.

**2. Specific for its purpose**

Organisations must be open about their reasons for obtaining personal data and what they plan to use it for. They should only use the personal data for the purpose they originally said it would be used for. This means that a company should not use the data to market other companies to their customers unless the individual has agreed to it. For example, if a local toy store starts selling children’s bikes, it is probably fine for them to market the bikes to existing customers. However, unless they have agreed, the toy store cannot use their customers’ details to promote other companies. They also shouldn’t pass customers’ details onto third parties unless they have already consented.

**Changes under GDPR**

Genetic and biometric information is now considered sensitive data, meaning that organisations may only request such information if it is required for a relevant purpose. A health clinic, for example, should require such information in order to provide the best possible care for their patients.

**3. Be adequate and only for what is needed**



The data you hold on your customers should be adequate for the purpose you are holding the information. You should avoid holding more information than necessary for your customers. The best practice is to calculate the information you need in order to achieve your goals, a practice known as “minimisation”. An example of this would be when an individual unsubscribes from a service. In this case, the company should only keep hold of the minimum information needed in order to hold records on former customers.

**Changes under GDPR**

Privacy notices or “how we use your information” guides now need to be clearer than before. This means that mere consent is not enough; the individual must be informed of exactly what their data is being used for. Further, organisations must inform the person of their right to withdraw consent at any time.

**4. Accurate and up to date**

Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate. When a customer updates the information a company holds on them, the organisation must stop contacting the individual using the previously provided details. Moreover, organisations should not simply wait for individuals to contact them to update their information, rather they should be active in ensuring they have the correct information on an individual.

For example, a company that sells books to individuals online doesn’t need to regularly check they have the correct information about them. However, if a company awards a pay increase to a staff member, their details and salary should be checked and updated where necessary.

**5. Not kept longer than needed**

Organisations must regularly review the length of time they retain data on individuals. Only holding on to data for the amount of time required will make it easier to manage your data and provide personal information to customers that request it. Data that is out of date or no longer necessary must be properly destroyed or deleted. For example, a customer contacts a music store to tell them they no longer wish to receive any marketing information and to remove their details from their records. The company should retain enough information on the individual to ensure they can remove them from their marketing lists.

**6. Take into account people’s rights**

People have the right to access their personal data, stop it from being used if it is causing distress, prevent it from being used for direct marketing, have inaccurate data changed, and claim compensation for damaging data breaches. In certain cases, customers have the right to request that specific data be deleted or destroyed. Customers should only request information relevant to themselves. The organisation has a responsibility to establish whether the information requested by customers is relevant to the person requesting it.

Customers can also request to see the information held on them by submitting a subject access request. This is a request typically sent by email, fax or post. While organisations can issue an online form for individuals to request they stop holding information on them, they shouldn’t require this as the only way to do so.

**Changes under GDPR**

A new “right to be forgotten” in the GDPR means that someone can request that online content is removed from an organisation’s database. **The Data Portability Act**means that a person can request all their personal data be transfered to another system for free. For example, they may wish to have all their photos transfered from one social network to another.

**7. Kept safe and secure**

A proper physical and technical security system must be used to keep personal information safe and secure, and not be exposed to undue security risks. It is advisable to provide training for staff in your organisation on data protection and cyber security. Further, your information security system should be relevant to the nature of your business and the data you hold on your customers. For example, a bank should have a higher information security system than a local book store. This is because the potential repercussions of a data breach stand to be much higher than for the book store.

**Changes under GDPR**

Companies that process over 5,000 personal records per year and employ over 250 employees are now required to appoint a Data Protection Officer, or DPO. The DPO is responsible for everything related to keeping personal data secure and cannot be easily replaced. Appointing someone in this position means personal data can be kept safe and secure more easily, with customer and employee rights being respected according to GDPR.

**8. Not be transferred outside the EEA**

Data should not be transferred to other countries that do not have the same level of data protection. For example, with the US, the EU has a ‘Privacy Shield’ that American companies can sign up for to enable data to be legally sent across the Atlantic. Data sent within the EEA and a few other specified countries is allowed.

**Changes under GDPR**

Organisations must receive explicit consent from their customers for their personal information to be transferred outside of the EEA. GDPR can still hold a company liable even after data has been transferred to another country. These changes mean that companies must consider the impact GDPR could have on their international data transfers.