

GUIDE TO THE GDPR



**What is the GDPR?**



THE FINAL

C

O

U

N

T

D

O

W

N

25th May 2018

**The General Data Protection Regulation (GDPR) will come into effect on 25th May 2018 and is essentially an updating of the current EU Data Protection Directive which was enacted in the UK as the Data Protection Act 1998. It constitutes a major overhaul of Data Protection legislation, and the UK government has confirmed that the UK’s exit from the EU will not affect its enforcement. It will be enacted in the UK under a new Data Protection Act 2018.**

The GDPR applies to all organisations which either control (“data controllers”) or process (“data processors”) personal data. Personal data refers to any information relating to an identifiable living person who can be directly or indirectly identified by reference to an identifier (such as their name, an identification number or an online identifier), or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. The legislation applies to both automated personal data and manual filing systems.

**Data protection principles**

There are 6 overarching data protection principles, which establish that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner which is inconsistent with those purposes

25th May 2018

1. Adequate, relevant and limited to what is necessary
2. Accurate, and where necessary, kept up to date
3. Kept in a form which permits identification of data subjects for no longer than is necessary
4. Processed in a manner that ensures appropriate security of the data

**Lawful basis for processing**

Organisations must have a valid basis for processing personal data, of which there are six.

The first is where the individual has given informed **consent**. This must be unambiguous and involve a clear affirmative action (an opt-in). Where consent is not the lawful basis, processing will be lawful only if it is necessary for:

1. the performance of a **contract** to which the subject is a party or because the subject has asked the organisation to do something before entering into a contract (e.g., provide a quotation)
2. compliance with a **legal obligation** to which the organisation is subject
3. the protection of the **vital interests** (life) of the subject or another person
4. the performance of a t**ask** **carried out in the public interest or the exercise of official authority**.
5. the purposes of the **legitimate interests** pursued by the organisation, except where these are overridden by the interests or fundamental rights and freedoms of the data subject.

There may be more than one lawful basis for a particular processing activity, but the important thing to remember is that they must be documented in order to show compliance. Furthermore, it is not open to the organisation to change the lawful basis for a given processing activity. This is particularly important if consent is relied upon, as consent can be withdrawn at any time, leaving the organisation unable to continue processing.

**Relying on consent**

The GDPR sets a much higher standard for valid consent than is the case with the current DPA. Consent must be

* requested in an intelligible and easily accessible form, using clear and plain language, and in a manner which is clearly distinguishable from other matters
* unambiguously given, involving a clear affirmative action
* freely given - the organisation must not be in a position of power over the individual
* given for each distinct processing operation (“granular” consent)
* not generally be a condition of signing up to a service

Data subjects have a specific right to withdraw consent once given, and the organisation must make it easy for them to do so.

Consent is appropriate if the organisation can offer people genuine choice and control over how it uses their data, and wants to build trust and engagement. If genuine choice cannot be offered, consent is not the appropriate legal basis.

**Special category data**

The GDPR specifies certain types of data as “special category” and imposes extra requirements in relation to the lawful basis for processing them. These special categories relate to information about:

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Health
* Sex life or sexual orientation
* Genetic or biometric data

In order to lawfully process such data, an organisation must be able to rely on a lawful basis for processing as set out above, and also a **condition for processing** from one of the following:

1. The subject has given explicit consent;

Or, processing is:

1. necessary for the purposes of carrying out obligations and exercising specific rights the organisation or subject has in the field of employment and social security or protection law
2. necessary to protect the vital interests of a person where the subject is physically or legally incapable of giving consent
3. carried out in the course of the organisation’s legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
4. relates to data which are manifestly made public by the subject
5. necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
6. necessary for reasons of substantial public interest
7. necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care treatment or the management of health or social care systems and services
8. necessary for reasons of public interest in the area of public health
9. necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

**Criminal offence data**

In order to lawfully process data about criminal convictions or offences an organisation must have both a lawful basis for processing, as set out above, and either a legal or official authority for the processing. This would appear to mean that carrying out routine criminal records checks on employees will only be lawful where an organisation is recruiting to a role for which such checks are required by law, e.g., roles involving working with vulnerable adults or children where a DBS check is required. However, the Government has stated its intention to legislate to authorise the use of such checks by other organisations, provided that they have satisfactory procedures and safeguards in place. It will also authorise the processing of criminal records data where the subject has given his or her consent. This will be legislated through the Data Protection Bill 2017.

**Individual rights**

Individuals have certain rights in relation to their personal data. These are to

1. Be Informed about the data– the organisation must supply specific information including the purpose of the processing and the lawful basis for it, any recipient or categories of recipients of the data, details of transfers to third countries and safeguards, the retention period for the data, the source the personal data originates from, and the data subject’s rights. If data is obtained from the individual directly, this information must be provided at the time the data is obtained. This is known as a **Privacy Notice** (see below).
2. Access their personal data – where requested, the organisation must provide the individual with access to their data, within one month of the request. The organisation cannot impose a charge unless the request is “manifestly unfounded or excessive”.
3. Rectification – individuals have the right to have inaccurate or incomplete data rectified, usually within one month of request.
4. Erasure – The right to have data erased applies where:

* there is no compelling reason for the continued processing of the data, i.e., where the data is no longer necessary for the purposes for which it was collected;
* when the individual withdraws consent (if consent is the legal basis);
* when the individual objects and there is no overriding legitimate interest for continued processing;
* when the data has been processed unlawfully (i.e., in breach of the GDPR);
* it is required to comply with a legal obligation.

The right does not apply in certain circumstances, the most relevant to private organisations being where the data is being processed for the exercise or defence of legal claims.

1. To restrict processing – when processing is restricted, the organisation will be required to store the data but not to further process it. This will apply where the individual contests the accuracy of the data, where the individual has objected to the processing and the organisation is considering whether its legitimate interests override the objection, where processing is unlawful or where the organisation no longer needs the data but the individual requires it to establish, exercise or defend a legal claim.
2. Data Portability – this gives individuals the right to have their data provided to them in a structured, commonly used and machine-readable format and to transmit it to another controller without hindrance. An example of this would be banking information. The right only applies where processing is carried out by automated means, and on the basis of consent.
3. Object – Individuals can object to processing in certain circumstances. The organisation can reject the request if it can demonstrate compelling legitimate grounds for the processing which override the interests of the individual, or if the processing is for the establishment, exercise or defence of legal claims.

The GDPR also gives individuals certain rights in relation to automated decision making undertaken by or on behalf of the organisation, including profiling (i.e., making a decision solely by automated means without any human involvement). An organisation can only undertake such processing where it is necessary for entry into or performance of a contract, authorised by law or based on the individual’s explicit consent. An example of profiling would be using online psychometric tests to *automatically* shortlist job applicants.

**Documenting data processing activities**



Organisations processing personal data will be required to maintain a written record of their processing activities which contains specific information including:

* the name and contact details of the organisation
* the purposes of the processing
* a description of the categories of data subjects and categories of data
* the categories of recipients to whom the personal data may be disclosed
* any transfers to a third country or international organisation
* the envisaged time limits for erasure of different categories of data
* a description of the technical and organisational security measures in place to protect the data.

**Privacy notices**

Where an organisation collects personal data directly from the data subject, it must provide the subject with the following information:

1. the identity and contact details of the organisation, and, if applicable, its representative
2. the contact details of the Data Protection Officer (DPO) if applicable (see below)
3. the purposes of the processing and the legal basis for it
4. the legitimate interests of the organisation (if this is the legal basis relied upon)
5. the recipient, or categories of recipients, of the data
6. the fact that the organisation intends to transfer data to a third country or international organisation, if applicable
7. the period for which the data will be stored, or the criteria used to determine that period
8. the individual’s rights in respect of the data, including the right to withdraw consent where applicable
9. the individual’s right to lodge a complaint with a supervisory authority
10. whether the provision of data is a statutory or contractual requirement, or necessary to enter into a contract, as well as whether the individual is obliged to provide the data and of the possible consequences of failure to provide it
11. the existence of any automated decision-making, including profiling, and meaningful information about the logic involved and the envisaged consequences of such processing

The information must be provided to the individual in writing, or by other means (including electronically) at the time when the data is obtained. It must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed to a child.

Where the organisation is obtaining personal data from a third party, the information it needs to provide to the individual is very similar, and it must be provided within a reasonable period after obtaining the data, but at the latest, within one month. If the data is to be used to communicate with the individual, the information must be provided by the time of the first communication. If data is to be disclosed to another recipient, the information must be provided at the latest when the data is first disclosed.

**Data Protection Impact Assessments (DPIAs)**

When an organisation is preparing to process information in a new way, in particular using a new technology, and where this is likely to result in a high risk to the rights and freedoms of individuals, it must carry out an assessment of the impact of the envisaged processing on the protection of the data (DPIA). This is required in particular in the case of

* any systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling
* processing on a large scale of ‘Special Category’ data (see above) , or of data relating to criminal convictions
* systematic monitoring of a publicly accessible area on a large scale (CCTV)

The DPIA should contain a description of the processing and its purpose, an assessment of the necessity and proportionality of the processing, an assessment of the risks to individuals in relation to their data, and details of the measures in place to address the risk.

**Contracts with data processors**



Whenever an organisation uses a third party to process personal data on its behalf, it must have a written contract in place with that party. This is a new requirement under the GDPR which does not feature in the current Data Protection Act.

The contract must include the following details:

* the subject matter and duration of the processing
* the nature and purpose of the processing
* the type of personal data and categories of data subject
* the obligations and rights of the data controller

and state that the data processor must:

* only act on the written instructions of the controller
* ensure that people processing the data are subject to a duty of confidence
* take reasonable measures to ensure the security of processing
* only engage a sub-processor with the prior consent of the data controller and a written contract
* assist the data controller in providing subject access and allowing data subjects to exercise rights under the GDPR
* assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and DPIAs
* delete or return all personal data to the controller as requested at the end of the contract
* submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting obligations, and tell the controller immediately if it is asked to do something which infringes the GDPR

The organisation must have a written contract in place with every other party who processes personal data on its behalf, e.g. payroll bureaus, recruitment agencies, occupational health providers, etc.

Organisations who process personal data on behalf of another organisation must have their own contracts in place with any organisation that in turn processes such data on their behalf.

**International transfers of data**

Personal data cannot be transferred outside the EU unless where the European Commission has decided that a third country or territory, or an international organization, ensures an adequate level of protection (currently this list includes Argentina, Israel, New Zealand and Switzerland. The full list is available on the EU Commission website) . However, data may be transferred where the organisation receiving the data has provided adequate safeguards in the form of either:

* a legally binding agreement between public authorities or bodies;
* binding corporate rules governing transfers made between organisations within a corporate group (*note that there are stringent requirements with regard to such rules*)

Such transfers may also be undertaken where the transfer is:

* made with the individual’s informed consent;
* necessary for the performance of a contract between the individual and the organisation, or which is made in the interests of the individual;
* necessary for important reasons of public interest;
* necessary for the establishment, exercise or defence of legal claims;
* necessary to protect the vital interests of the individual or other people, where the individual is physically or legally incapable of giving consent.

One-off, or infrequent, transfers of data concerning only a relatively few individuals may also be made (except by a public authority) where they are necessary for the purposes of the compelling legitimate interests of the organisation, which are not overridden by the interests of the individual, and where they are subject to suitable safeguards put in place by the organisation to protect the data. In such situations the organisation must inform the relevant supervisory authority (ICO) of the transfer and provide additional information to the individuals.

****

**Dealing with data breaches**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, e.g.,



* access by an unauthorised third party
* sending data to an incorrect recipient
* losing computer devices which contain personal data
* alteration of personal data without permission

If as result of a breach it is likely that there will be a risk to an individual’s rights or freedoms, the data controller must inform the ICO within 72 hours. If the organisation determines that there isn’t sufficient risk to inform the ICO, it should still document its decision in order to provide evidence. If the breach is by an organisation which processes the data on behalf of another organisation, the processor must inform the controller, who must inform the ICO.

In addition, if the breach is likely to result in a high risk to the rights and freedoms of an individual, the organisation must inform the individual concerned directly and without undue delay. This notification should provide the name and contact details of the DPO or other contact point, the nature and likely consequences of the breach and the measures the organisation is taking or proposes to take to deal with the breach and mitigate its consequences.

**Ensuring data security**

Organisations are required to demonstrate that they comply with the principles set out in the GDPR, in particular by implementing appropriate technical and organisational measures to ensure data security. What is appropriate will depend upon the nature of the processing activities, and the size of the organisation, but for most organisations who process personal data on a day to day basis such measures are likely to include the following:

* encryption of data and devices
* use of effective passwords
* restricting access to data to certain individuals
* ensuring data can be restored in a timely manner in the event of an incident
* Regularly testing, assessing and evaluating the effectiveness of security measures

Organisations should also implement internal data protection policies, train staff in how to adhere to them, review all HR Policies to ensure that they support data protection principles and implement regular internal security audits to demonstrate compliance.

**Data Protection Officers (DPOs)**

The organisation must appoint a DPO if it:

1. is a public authority; or
2. carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
3. carries out large scale processing of Special Categories of data or data relating to criminal convictions and offences

The role can be given to someone within an organisation, or to an external third party, but the DPO must operate independently and report to the highest level of management in the organisation. The DPO does not require special qualifications or credentials, but must have professional experience and knowledge of data protection law, proportionate to the type of processing the organisation carries out, and be provided with adequate resources to enable them to meet their obligations.

Organisations may still elect to have a DPO, even if they are not required to do so under the legislation, as this will assist them in meeting their obligations and demonstrating compliance.

**For further help and assistance in relation to ensuring that your organisation complies with its obligations under the GDPR, please contact EML on**

**01942 727200,**

**or email us at**

**eml@employeemanagement.co.uk**