GDPR Policy and Procedure

The GDPR Policy and Procedure for minc people

Chief People Officer
people@mincgroup.co.uk

Contents

Introduction

The European Union's General Data Protection Regulation (GDPR) comes into force in the UK on 25th May 2018 to replace the Data Protection Act (DPA) 1998. Many of the GDPR's main concepts and principles are much the same as those in the Data Protection Act, however the GDPR will bring in stricter obligations on employers relating to holding personal data, and significant enhancements on individual's rights that all employers must adhere to.

GDPR Key Principles

The key Data Protection principles set out the main responsibilities for organisations and requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

minc people (the company) is committed to ensuring personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Lawful Basis for Processing

The six lawful bases for processing are set out in full in Article 6 of the GDPR. No single basis is "better" or more important than the other, and at least one of these must apply whenever personal data is processed:

- Consent;
- Contractual Agreement;
- Legal Obligation;
- Vital Interests;
- Public task;
- Legitimate Interests (of your organisation or the legitimate interest of a third party).

In general, minc people relies on the individual's consent to process their data. Where there are exceptions such as a legal obligation, contractual agreement or legitimate interest they will be stated in the company's privacy policy held on the company website.

Rights of the individuals (data subject)

The GDPR provides the following rights for individuals:

- To be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

minc people provides full details of its privacy information through its privacy policy held on the company website. This privacy policy is reviewed and updated regularly, and any new uses of an individual's data will be made available to data subjects prior to these changes taking place.

Right of Access (including Subject Access Requests)

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing. Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Should an employee wish to have access to their personal data they should provide their request in writing to the Managing Director.

Under the GDPR there is no longer a fee for dealing with subject access requests and the information will be provided "free of charge" and without delay - no later than one month from the date of receipt of the initial request, unless the requests are numerous or complex in which case information will be provided within two months of the initial request.

minc people may charge a "reasonable fee" to comply with requests for further copies of the same information, or should a request be found to be manifestly unfounded or excessive, particularly if it is repetitive.

Should an access request be subject to a fee or delay, the company will write to the individual within one month of receipt of the initial request to explain why this is necessary.

On receipt of the data, should an individual find that their records are either inaccurate or incomplete, they should provide the company with a rectification request in writing to the Managing Director, to request having the data is rectified.

On receiving a request for rectification, the company will take reasonable steps to rectify the data if necessary, however should the company believe that the data is accurate, the individual will be contacted in writing of the company's findings, explanation of the decision not to amend the data, and right to make a complaint to the Information Commissioners Office (ICO) if necessary.

Right to erasure or to restrict processing

The GDPR introduces a right for individuals to have their personal data erased (the right to be forgotten) or to request for processing to be restricted.

These rights are not absolute and only applies in certain circumstances. Further information is available on the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Should an individual wish to have their personal data erased or restricted, they should provide their request in writing to the Managing Director.

minc people will respond in writing no later than one month from the date of receipt of the initial request.

The company has the right to refuse to comply with requests for restriction should the request be found to be manifestly unfounded or excessive, taking into account if the request is repetitive.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

This is a new right, and only applies to personal data an individual has provided to minc people where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.

Should an individual wish to have their personal data transmitted to another organisation, they should provide their request in writing to the Managing Director.

The company will respond in writing with undue delay but no later than one month from the date of receipt of the initial request, unless the requests are numerous or complex in which case information will be provided within a further two months of the initial request.

Should a request for data portability be subject to a fee or delay, the company will write to the individual within one month of receipt of the initial request to explain why this is necessary.

Should the company conclude that no action will be taken in response to a request, they will write to the individual, informing them of their right to complain to the ICO and to a judicial remedy without undue delay and at the latest within one month.

Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on "grounds relating to his or her particular situation". Should an individual object to their personal data being processed, they should provide their request in writing to the Managing Director.

minc people will cease any processing of personal data on receipt of the objection until the request is concluded and agreed unless:

- The company can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

Accountability

The accountability principle in Article 5(2) requires organisations to demonstrate that they comply with the principles and states explicitly that this is their responsibility.

Organisations must:

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default.

Measures could include:

- data minimisation;
- pseudonymisation;
- transparency;
- data minimisation;
- allowing individuals to monitor processing; and
- creating and improving security features on an ongoing basis;
- use data protection impact assessments where appropriate.

Organisations can also:

- adhere to approved codes of conduct and/or certification schemes

Data Protection Impact Assessments (DPIA's)

The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If a DPIA identifies a high risk which you cannot mitigate, the company must consult the ICO.

This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance. DPIAs are now mandatory in some cases, and there are specific requirements for content and process.

What is a DPIA?

A DPIA is a process to systematically analyse your processing and help you identify and minimise data protection risks. It must:

- describe the processing and your purposes;
- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk but should help to minimise risks and consider whether they are justified. A DPIA must be completed for processing that is likely to be high risk. An effective DPIA can also bring broader compliance, financial and reputational benefits, helping to demonstrate accountability more generally and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

When do we need to do a DPIA?

A DPIA must be completed before any type of processing begins which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed yet, it will require screening for factors which point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says a DPIA must be completed if minc people plans to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires a DPIA to be completed if minc people plans to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Completing a DPIA should be considered for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Do we need to consult the ICO?

If a DPIA has been carried out that identifies a high risk, and the company cannot take any measures to reduce this risk, then the ICO will need to be consulted (using the ICO's online form). Processing cannot go ahead until this has been done.

The focus is on the 'residual risk' after any mitigating measures have been taken. If the DPIA identifies a high risk, but measure have been taken to reduce this risk so that it is no longer a high risk, the ICO will not need to be consulted.

The ICO will generally respond with a written response advising whether the risks are acceptable or whether minc people will need to take further action within eight weeks (although this can be extended this by a further six weeks in complex cases).

International Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined, and minc people is fully compliant with these restrictions.

Breaches of GDPR

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the company will endeavour to inform those individuals without undue delay.

What is a personal data breach?

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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach

whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms will need to be established. If it's likely that there will be a risk, then the company must notify the ICO; if it's unlikely then the company does not have to report it. However, if decided that there is no need to report the breach, the company will need to be able to justify this decision, and as such should document it.

On becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen. If appropriate, in the first instance individuals should notify the Managing Director verbally and in writing who will work with the individual on ascertaining whether a report needs to be reported to the ICO.

If deemed necessary, companies must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If reporting is likely to take longer than this, minc people must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach. This can be found on the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if the organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So, Article 34(4) allows you to provide the required information in phases, if this is done without undue further delay.

When to tell individuals about a breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the company will inform those concerned directly and without undue delay.

minc people will provide individuals with the nature of the personal data breach and, at least:

- the name and details of the appointed data protection contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Raising Awareness

minc people is committed to ensuring its employees, consultants, subscribers, clients, suppliers and any other individuals that the company may hold data for are fully aware of how and why personal data is stored, where and for how long.

Full details can be found in the minc people privacy policy held on the company website.

Employees and Consultants

As part of the onboarding process, minc people will provide training to new employees or consultants on GDPR and the responsibilities of individuals working for or on behalf of the company.

The company will provide annual refresher training to all individuals working on or on behalf of the company.