bates weston
CHARTERED ACCOUNTANTS & BUSINESS ADVISORS

GENERAL DATA PROTECTION REGULATIONS MAY 2018

Contents

WHAT DO YOU NEED TO KNOW?

THE BASICS

- What is personal data?
  - Any information that can be used to directly or indirectly identify an individual. E.g. Name, reference number, location data, online identifier regardless of whether it is held digitally or manually.
  - There is a specific category of personal data, Sensitive Personal data, which includes genetic and biometric data.
- What are an organisation's main responsibilities under GDPR?
  - Personal data should be
    - Processed **lawfully, fairly** and in **a transparent** manner
    - Collected for **specified, explicit and legitimate** purposes and not further processed in a manner incompatible with those purposes (archiving for public interest, scientific or historical research or statistical purposes is not regarded as incompatible)
    - 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. Any inaccurate data must be rectified or erased without delay
    - Kept in a form which permits identification of data subjects **for no longer than necessary**
    - Processed in a manner that ensures **appropriate security** of the personal data, including unauthorised /unlawful processing, accidental loss, destruction or damage.

IN SUMMARY RELEVANT ACCURATE PERSONAL DATA SHOULD BE COLLECTED FOR A SPECIFIED LAWFUL PURPOSE, KEPT SECURELY AND FOR NO LONGER THAN NECESSARY.

WHAT IS A LAWFUL PURPOSE?

If you can achieve the same purpose without processing data, you will not have a lawful basis.

Here are the 6 lawful bases for processing data:

1. CONSENT: The individual has given clear consent for you to process their personal data for a specific purpose
2. CONTRACT: The processing is necessary for a contract you have with an individual, or because they have asked you to take specific steps before entering into a contract
3. LEGAL OBLIGATION: The processing is necessary for you to comply with the law
4. VITAL INTERESTS: the processing is necessary to protect someone's life
5. PUBLIC TASK: the processing is necessary for you to perform a task in the public interest or for your official lawful function
6. LEGITIMATE INTEREST: the processing is necessary for your legitimate interests or the legitimate interests of a third party

Once you have decided on your lawful purpose, you must demonstrate that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You will also need to produce a privacy notice. This will include information about your intended purposes for processing the personal data and the lawful basis for processing. This applies whether you collect the data personally or from another source.

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

WHAT ARE THE INDIVIDUAL'S RIGHTS?

The GDPR provides the following rights for individuals:

1. **The right to be informed** – a privacy notice must include contact details for controller, purpose and lawful basis of processing, any recipients of data, if transferred to a third country safeguards in place, retention periods, data subject's rights, right to withdraw consent, right to lodge a complaint with a supervisory authority, contractual requirement, automated decision making if relevant. This information must be provided at the time the data are obtained.
2. **The right of access** - to their personal data and supplementary information. They have the right to obtain confirmation that their data is being processed, access to their data and information in the privacy notice. Information should be provided free of charge and within one month of receipt of the request at the latest. Begin by verifying the identity of the person making the request.
3. **The right to rectification** – for inaccurate or incomplete data within one month. If data is then used by others you must advise them of the rectification.
4. **The right to erasure** – to be forgotten – where there is no compelling reason for the continued processing of the data. Examples include where consent is withdrawn, where data is no longer necessary in relation to the purpose for which it was originally collected, no overriding legitimate interest, unlawfully processed in the first place or there is a legal obligation to erase. You can refuse to erase to exercise the right to freedom of speech, to comply with a legal obligation of public interest (public health, scientific research, statistical purposes) or defence of legal claims. Where you have passed the erased data on – you must advise those parties of the erasure.
5. **The right to restrict processing** – restrict processing where an individual contests accuracy of data, objected to the processing, where processing is unlawful, if you no longer need the data but the individual requires it to establish, exercise or defend a legal claim. You must advise others to whom you have disclosed this data of the restriction.
6. **The right to data portability** – allows individuals to obtain and reuse their personal data for their own purposes across different services, moving copying or transferring data easily from one IT environment to another in a safe and secure way. It only applies to personal data an individual has provided to a controller on the basis of consent or contract and when processing is automated.
7. **The right to object** – to processing based on legitimate interests, public interest, direct marketing and scientific/historical research and statistics. You must stop processing the data as soon as you receive an objection – without exception.
8. **Rights in relation to automated individual decision making and profiling** (automated processing of data to evaluate certain things about an individual) – GDPR does apply plus additional provisions. AID only when necessary, authorised by EU law, or based on explicit consent, must identify that processing falls under Article 22, introduce ways for them to request human intervention, carry out regular system checks.

ACCOUNTABILITY AND GOVERNANCE

You are expected to have comprehensive but proportionate governance measures. These measures should minimise the risk of breaches and uphold the protection of personal data. Adequate policies and procedures must be in place.

Demonstrate compliance by

- Internal data protection policies
  - Staff training
  - Internal audits of processing activities
  - Review HR policies
- Maintain relevant documentation on processing activities
- Where appropriate appoint a data protection officer
- Protect data by design and default
  - Data minimisation
  - Pseudonymisation
  - Transparency
  - Allowing individuals to monitor processing
  - Creating and improving security features on an ongoing basis
- Use data protection impact assessments where appropriate

Data controllers must:

HAVE CONTRACTS WITH 3RD PARTY PROCESSORS

1. The contract in place must be GDPR compliant
2. **Controllers must only appoint processors who can provide sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected.**

DOCUMENT PROCESSING ACTIVITIES

1. Maintain up to date, written, electronic records on processing data, data sharing and retention
2. Make the records available to ICO on request
3. For SMEs documentation requirements are limited to certain types of processing
4. Information audits can be helpful in documenting processes

DATA PROTECTION IMPACT ASSESSMENTS

(Also known as Privacy Impact Assessments or PIAs). An effective assessment will allow an organisation to identify the most effective way to comply with their data protection obligations and meet an individual's expectation of privacy.

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

DO I NEED A DATA PROTECTION OFFICER?

Yes, if you are a public authority, carry out large scale systematic monitoring of individuals, carry out large scale processing of special categories of data or data relating to criminal convictions and offences. You may choose to appoint a DPO as best practice. The role involves:

- Inform and advise organisation and its employees about their obligations to comply with GDPR and other data protection laws
- Monitor compliance with GDPR, manage internal data protection, advise on Data Protection Impact assessments, train staff and conduct internal audits
- First point of contact for supervisory authorities and individuals whose data is processed
- Reports to board, operates independently and adequately resourced

DO I NEED A CODE OF CONDUCT AND CERTIFICATION?

- They help to demonstrate compliance
- Improve transparency and accountability
- Provide mitigation against enforcement action
- Improve standards by establishing best practice

BUT

- They are subject to mandatory monitoring
- Valid for three years

THE DATA PROTECTION FEE

Paid by organisations to fund the ICO.

1. Tier 1 – micro organisations. This applies if you have a maximum turnover of £632,000 for your financial year or no more than 10 members of staff. The fee for tier 1 is £40.
2. Tier 2 – small and medium organisations. This applies if you have a maximum turnover of £36 million for your financial year or no more than 250 members of staff. The fee for tier 2 is £60.
3. Tier 3 – large organisation. If you do not meet the criteria for tier 1 or tier 2, you have to pay the tier 3 fee of £2,900.

   Some organisations are exempt.

   https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

SECURITY

Data must be secure. It must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage by appropriate technical and organisational measures.

INTERNATIONAL TRANSFERS

There are restrictions on transferring personal data outside the EU, to third countries or international organisations. If the organisation receiving the data has adequate safeguards the data may be transferred.

PERSONAL DATA BREACHES

- Certain types of data security breaches must be reported to the relevant supervising authority within 72 hours, chiefly if there is a risk of adversely affecting individual's rights and freedoms. In addition, you must inform the individuals without delay. Records of breaches must be maintained.
    - Examples of data breaches include **– LOSS, DESTRUCTION, CORRUPTED OR DISCLOSED**
        - Access by unauthorised third party
        - Deliberate or accidental action/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
        - Loss of availability of personal data
- Robust breach detection, investigation and internal reporting procedures must be in place.

DEFINITIONS

- You are a data controller if you determine the purpose and the means of processing personal data. You must ensure that your contracts with processors comply with GDPR.
- You are a processor if you process personal data on behalf of a controller. You will have legal liability if you are responsible for a breach.
- The GDPR applies to both controllers and processors.
- It does not apply to processing carried out by individuals purely for personal/household activities.

(ICO, 2018)

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