GDPR
General Data Protection Regulation

Preparing for 25th May 2018

Contents

General Data Protection Regulation 2
Introduction 2
Definitions 3
Children 3
Types of data: 4
Lawful processing conditions of personal data (legal basis) 4
Principles of GDPR 5
Consent 6
Methods of Obtaining Consent 6
Alternatives to Consent 6
Preparing for GDPR – 10 tips 7
Self-help checklist on GDPR 9
MAIN RESPONSIBILITIES 9
Rule 1: Fair obtaining: 9
Rule 2: Purpose specification 9
Rule 3: Use and disclosure of information 9
Rule 4: Security 9
Rule 5: Adequate, relevant and not excessive 10
Rule 6: Accurate and up-to-date 10
Rule 7: Retention time 10
Rule 8: The Right of Access 10
Registration 10
Training & Education 10
Co-ordination and Compliance 11

General Data Protection Regulation

General Data Protection Regulation replaces existing law in all member states on 25 May 2018 and is designed to result in single, uniform set of data protection rules applying across the EU

Areas of key concern:

- outsourcing implications including international transfers within and outside EEA
- data protection/privacy notices and methods of consent
- record of processing operations/data inventory
- the role of the Data Protection Officer

Introduction

Data protection laws arose from concerns over individuals' right to privacy as increasing amounts of personal information was gathered by businesses and other organisations throughout the 20th century.

Digital technology has changed the way many organisations operate and the evolving means of collecting, storing and processing personal data means that laws needed to be changed to keep pace. GDPR accounts for modern methods of capturing and processing people's data and takes steps to ensure people have sufficient control over their own information.

NB: Data protection is not just about digital information, but all personal information that is stored.

GDPR protects individuals, not organisations.

The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The new regulation allows individuals to request access, corrections and removal of their personal information in ways that weren't available before.

The new regulation requires clear evidence of consent from individuals.

Definitions

- Data subject
    - Refers to an individual whose personal information is the data in question
- Processing
    - The collection, storing, and transferring of personal data
- Profiling
    - Often done by larger organisations and involves automatic processing of personal information to evaluate aspects of the individuals' behaviour in order to make decisions or take action
- Data Protection Commissioner
    - Ireland's independent authority set up to uphold information rights in the public interest.
- Data Controller
    - The person within an organisation that decides what data is collected, what it's used for and who it is shared with.
- Senior Information Rights Owner (SIRO)
    - A member of the Board who oversees data policies
- Data Protection Officer
    - This role is required in certain circumstances such as public authorities and where organisations deal with sensitive data
- Data Processor
    - Anyone who processes data on the instruction of your Data Controller
        - This could be a third party organisation or business

Children

With regards to children, GDPR enhances the protection of children's personal data.

Any privacy notes for services offered directly to children must be written in clear, simple language.

A child under 16 cannot give consent themselves. This is required from a person holding 'parental responsibility' (parent/guardian).

Types of data:

- **Personal data**
    - Information that relates directly to an individual. Exp: name, phone number, email, photos, genetic data, economic data.
    - **This kind of data is the focus of GDPR and data protection.**
- Anonymous data
    - Data which cannot be traced back to the original individual but can still be used for research purposes.
    - NOT covered by GDPR as it is not traceable.
- Pseudonymous data
    - Data which has been written under a false name (pseudonym) but can still be connected back to an individual using a specific code.
        - This acts as an extra layer of security.
    - This is covered under GDPR as it is considered personal data and the person can be identified.

Lawful processing conditions of personal data (legal basis)

There are six valid reason for processing personal information.

1. Consent
    a. The data subject has clearly and willingly agreed to the processing of their personal data.
        i. This is probably the most relevant one for IAYO members
2. Contract
    a. Processing of personal data is necessary for the performance of a contract or prior to the owner of the data entering into a contract
3. Legal obligation
    a. If processing is necessary due to legal obligations (for example, if the data controller is obliged to notify Túsla where they become aware of allegations of child abuse)
4. Vital interests
    a. If the processing of personal data is necessary in order to protect the vital interests of the data owner
5. Public interest/official authority
    a. If the processing of personal data is necessary for a task to be carried out in the public interest or in the exercise of an official, regulatory or statutory authority vested in the Controller (for example, where a non-profit is acting as an agent for the Dept. of Social Protections in providing a service)
6. Legitimate interest
    a. If the processing of personal data is necessary for the purposes of the legitimate interests pursued by the Data Controller and Data Protector,

except where they are over ridden by the interests of fundamental rights of the Data Subject, especially if they're a child.

Principles of GDPR

GDPR principle lays out six principles for processing personal data

1. Lawfulness, fairness and transparency
    a. Data should be gathered and used in a way that is legal, fair and understandable. The public have a right to know what is being gathered and have this corrected or removed
2. Purpose limitation
    a. Data should only be used for legitimate purposes specified at the time of collection.
    b. This data cannot be shared with third parties without permission
3. Data minimisation
    a. Data collected should be limited to only what is required for the purpose stated
    b. Organisations should not collect data en masse without a clear purpose
4. Accuracy
    a. Personal data stored should be accurate, up to date.
    b. If it is no longer accurate, it should be rectified or erased.
5. Storage limitation
    a. Personal data should only be stored for as long as is necessary.
        i. "the data shall not be kept for longer than is necessary for that purpose or those purposes"
        - section 2(1)(c)(iv) of the Act
    b. Data can be archived securely and used in the future
    c. Where possible, personally identifiable information should be removed to leave anonymous data.
6. Integrity, security and confidentiality
    a. Personal data should be held in a safe and secure way. Steps should be taken to ensure this security and avoid accidental lost, misuse or destruction of information.
7. Liability and accountability
    a. Those in charge of the personal data (Data Controller or Data Protector) will be required to show their compliance with GDPR.
    b. The Data Controller will ensure that the Data Protector carries out data processing in strict compliance with GDPR

Consent

Methods of Obtaining Consent

Article 6(1) –legal basis for processing:

- Freely given, specific, informed and unambiguous
- Should not be bundled with other consents
- Intelligible, easily accessible, clear and plain language
- Ban on pre-ticked boxes
- Right to withdraw at any time
- Provision of a service must not be made conditional on consent to non-essential forms of processing

Alternatives to Consent

- Article 6(1) -processing necessary for one of the following purposes:
    - the performance of a contract to which the data subject is party
    - for compliance with a legal obligation imposed on the controller
    - to protect the vital interests of the data subject/other person
    - for the performance of a task carried out in the public interest or in the exercise of official authority
    - for the legitimate interests of the controller/third party –subject to fundamental rights/freedoms of data subject

Preparing for GDPR – 10 tips

1. Ensure that the key personnel in your organisation are fully **aware** that the GDPR law is changing and start factoring this into future planning.
2. You should designate someone to take **responsibility for data protection compliance** and figure out where this role will sit in your organisational structure.
3. **Assess** your current data management processes and **become accountable** by identifying all types of data processing activities by checking:
    a. What personal data was obtained from Data subject?
    b. Why was it sought and what consent was given by Data Subject?
    c. How was it originally gathered?
    d. As per the **Principles of GDPR**, is the data kept accurate and up to date?
    e. How long will the data be retained?
        i. "the data shall not be kept for longer than is necessary for that purpose or those purposes"
        - section 2(1)(c)(iv) of the Act
    f. How secure is it in terms of encryption and accessibility?
    g. Do you share it with third parties and on what basis might you do so?
        i. Do they know the retention period and contractual obligations?
        ii. "the data shall not be kept for longer than is necessary for that purpose or those purposes"
        - section 2(1)(c)(iv) of the Act
4. **Review all your current data privacy notices** (for example, any declarations on forms that must be filled in by the data subject or their parent/guardian).
    a. **Identify any gaps** that may exist between the level of data collection and processing of this data and identify how you have made your customers, staff and service users aware of this collection. If a gap exists in your current system, readdress it using the guidelines in Step 2.
    b. **Note:** Before gathering any personal data, you must **notify the data subject** of the following:
        i. Your identity
        ii. Your reasons for gathering information
        iii. The use it will be put to
        iv. Who it will be disclosed to
        v. If it going to be transferred outside the EU
        vi. Legal basis for processing the data (see point 4)
        vii. How long you will hold on to the data
        viii. Their individual rights under GDPR (see point 5)
        ix. Their right of complaint where the individual are unhappy with the implementation of any of the above criteria
5. **Establish the legal basis and consent**
    a. You will have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request
    b. Usually for our members will be using ‘Consent’ and ‘Contractual’

        i. **See: Lawful processing conditions of personal data**
6. **Individual rights/Privacy rights under GDPR** – an organisation should review its procedures to ensure they cover all the rights individuals have, including, how you would delete personal data or provide data electronically and in a commonly used format. Rights for individuals under GDPR are:
    a. Subject access
    b. To have inaccuracies corrected
    c. To have information erased
    d. To object to direct marketing
    e. To restrict the processing of their information, including automated decision-making
    f. Data portability
7. Review and update your current procedures and plan how you will handle **data access requests** from third parties within the new laws.
    a. In most cases you will not be able to charge for complying with a request
    b. You will have a month to comply, rather than the current 40 days.
    c. You can refuse or charge for requests that are manifestly unfounded or excessive.
    d. If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.
    e. This should not affect our member organisations that much.
8. Review how to seek consent for information. **Consent** must be 'freely given, specific, informed and unambiguous'. Essentially, your individual cannot be forced into giving consent or be unaware that they are consenting.
    a. They must know exactly what they are consenting to.
    b. **NB:** Obtaining consent requires a positive indication of agreement
        i. It cannot be inferred from silence, **pre-ticked** boxes or inactivity.
9. **Processing children's data –** If the work of your organisation involves the processing of data from underage subjects, you must ensure that you have a system in place to gather consent from parents/guardians.
    a. **NB:** GDPR introduces special protections for children's data, particularly in the context of social media and commercial internet services.
    b. Consent needs to be verifiable, and therefore communication to your underage person in language they can understand.
10. **Reporting data breaches** – You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
    a. GDPR will introduce mandatory breach notifications if a personal data breach occurs in your organisation. All breaches must be report to the Data Protection Commissioner within 72 hours.
    b. Breaches that relate to identity theft or breach of confidentiality must be reported to the individual concerned.
    c. Failure to report a breach when required could result in a fine.

Self-help checklist on GDPR

Remember, you should be able to answer YES to all of the questions below. If you can, your organisation is in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

MAIN RESPONSIBILITIES

Rule 1: Fair obtaining:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them?
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with the Data Protection Commissioner, does our register entry include a proper, comprehensive statement of our purpose? *[Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]*
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Use and disclosure of information

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- If we are required to register with the Data Protection Commissioner, does our register entry include a full list of persons to whom we may need to disclose personal data? *[Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]*

Rule 4: Security

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?

- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorised people?

Rule 5: Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Rule 6: Accurate and up-to-date

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Rule 7: Retention time

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?

Registration

- Are we clear about whether or not we need to be registered with the Data Protection Commissioner?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? *[Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]*
- Is a named individual responsible for meeting our registration requirements?

Training & Education

- Do we know about the levels of awareness of data protection in our organisation?
- Are our staff aware of their data protection responsibilities - including the need for confidentiality?
- Is data protection included as part of the training programme for our staff?

Co-ordination and Compliance

- Has a data protection co-ordinator and compliance person been appointed?
- Are all staff aware of his or her role?
- Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?