

Complying with GDPR Requirements



- 02 December 2021
- Delivered by: Cork County PPN
- Facilitator: Caroline Egan, CramdenTECH Ltd.



Topics

- Bases for Processing Personal Data - Re-cap
- Obtaining, Recording and Managing Consent
- Data Protection Policy – general
- Data Protection Policy – HR implications
- Data Matrix
- Data Protection Framework
- Data Protection – Systematic Monitoring



The GDPR & Data Protection Act 2018– The Basics

- Data Protection Policy plus additional policies (information security & remote working)
- Privacy Statement
- Data Processing Log/Matrix
- Staff, Volunteer & Committee Member Training
- Analysis of data files/records – data retention periods
- Analysis of Emailing Marketing Database
- Put Data Processing Agreements in place with processors

Bases for Processing Data – Re-cap

- Necessary to enter into or perform a contract with a data subject
- Legal obligation to process the data
- Necessary to protect the “vital interests” of the data subject
- Necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest
- Data controller has a legitimate interest in processing
- Processing of health data for insurance or pension purposes (Ireland)
- Data subject has consented to processing



The GDPR Principles

1. Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
 - Data controllers are already required to process data fairly and lawfully. The GDPR now includes the principle of transparency.



The GDPR Principles

2. Data shall be 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.

- Data controllers must collect and process data for legitimate purposes. The GDPR does permit further processing of data however for public interest or scientific purposes.

The GDPR Principles

3. Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Data controllers are already required to ensure that the processing of data is not excessive relative to the purpose for which the data is being processed. The GDPR also makes it clear that the data controller should only process personal data that is necessary for the purpose for which it is being processed.



The GDPR Principles

4. Data shall be 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.

- Data controllers are required to at least take 'reasonable' steps to ensure that data is accurate and kept up to date.



The GDPR Principles

5. Data shall be 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.



The GDPR Principles

6. Data shall be 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.

- Data controllers should ensure that the technical and organisational measures are in place to ensure that data integrity and confidentiality are safeguarded.



The GDPR Principles

7. A data controller shall be responsible for, and be able to demonstrate compliance with the GDPR data protection principles.

- This GDPR emphasises the importance of data processing accountability. In other words, organisations must be able to show how they are complying with the data protection principles.



The GDPR – Rights of Individuals

1. The right to be informed

- Individuals have a right to information about how their personal data is processed by an organisation.
- Orgs should provide individuals with information about how their data is processed in a way that they can access and understand.



The GDPR – Rights of Individuals

2. The right of access

- The GDPR entitles individuals to obtain access to their personal data and to confirm that their personal data is being processed. Individuals are also entitled to access other relevant information, such as that contained in a privacy notice.
- Individuals are entitled to receive this information free of charge.

The GDPR – Rights of Individuals

3. The right to rectification

- If personal data is inaccurate or incomplete, individuals are entitled to have the data rectified.
- If an organisation has disclosed the inaccurate or incomplete data to a third party, they too must be informed of the rectification, where possible. The individuals should also be informed as to who the third parties are, where appropriate.



The GDPR – Rights of Individuals

4. The right to erasure

- The GDPR enables individuals to request the deletion or removal of personal data where there is no compelling reason for the continued processing of the data.

The GDPR – Rights of Individuals

Right to Data Erasure

Individuals have a right to have data erased in certain circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- The individual withdraws consent
- The individual objects to the processing and there is no legitimate reason for the organisation to continue processing the data
- The data was processed unlawfully
- The data must be erased to comply with a legal obligation
- Personal data is processed in relation to the offer of information society services to a child

The GDPR – Rights of Individuals

5. The right to restrict processing

- When data processing is restricted, an organisation is permitted to store the personal data but may not process it further.

Data processing restrictions apply in the following circumstances:

- Where individuals contest the accuracy of the personal data.
- When data processing is unlawful and the individual requests restriction rather than erasure.
- Where an organisation no longer needs the personal data, but the individual may do so to exercise, establish or defend a legal claim

The GDPR – Rights of Individuals

6. The right to data portability

Individuals may obtain and reuse their personal data for their own purposes across multiple services. This is referred to as data portability.

The right to data portability only applies when processing is carried out by automated means and:

- An individual has provided the personal data to a controller
- Processing is based on the individual's consent or for the performance of a contract.

The GDPR – Rights of Individuals

7. The right to object

Individuals have a right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing based on the exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific or historical research or statistical purposes

The GDPR – Rights of Individuals

8. Rights in relation to profiling and automated decision making

- The GDPR provides individuals with safeguards against the risk that a potentially damaging decision is taken without human intervention.
- Organisations must ensure that appropriate safeguards are also in place when processing personal data for profiling purposes. Profiling is used by many businesses and organisations to analyse and predict human behaviour, location and movements and personal preferences.



Using a Compliance Checklist

- Use a data protection compliance checklist to help map any compliance gaps!



Obtaining Consent – The Basics

Consent requests must be prominent, separate from other terms and conditions and easy to understand:

- the name of the organisation;
- the name of any third party controllers who will rely on the consent;
- why your organisation wants the data;
- what you will do with the data; and
- that individuals can withdraw consent at any time.

Recording and Managing Consent – The Basics

Remember to:



- Ask individuals to actively opt-in
- Give separate options to consent for different types of processing
- Keep consent records: who consented, when, how, and what they were told
- Make it easy for people to withdraw consent
- Keep consent under review – re-fresh consent where necessary – have a policy for reviewing consent

Obtaining Consent – Practical Scenario 1

When creating a sign-up pop-up for a website, remember to:

- Use clear language, outline content, frequency, channel
- Affirmative action to opt-in by clicking a sign-up button (Make sure any tick boxes are not confusing)
- Link to mailing terms and conditions where unsubscribe details are contained
- No incentives – no pre-conditions to signing up for a service unless it is necessary for that service (denial of services implications)

Sign up for our weekly News Bulletin today!



Get our weekly email of sector news and events direct to your inbox each Friday morning.

Read our full mailing consent T&C [here](#)

Obtaining Consent – Practical Scenario 2

When creating a simple registration form for a website, remember to:

- Use clear language, outline content, frequency, channel
 - Positive action required for sign up and mailing terms and conditions not bundled with service terms and conditions
1. Person inputs Name, Email and Password - required for service registration
 2. Tick box “I want to receive daily emails about funding opportunities in the non-profit sector
 “,
 3. “By continuing you are agreeing to our mailing terms and conditions, privacy policy, terms of service and billing terms.”

Obtaining Consent – Practical Scenario 3

Shopping Checkout Page:

Email Marketing Preferences

“ Yes, please – I want to receive daily targeted offers and promotions based on the products that I buy.

(Note: you will be able to unsubscribe at any time from all our emails.

[Here](#) are the full terms and conditions.)

Obtaining Consent – Practical Scenario 4

Website Contact Forms.

1. Fields of Data: Name, Organisation, Email, Subject, Message
2. Tick Box “ I accept that the data I input here will be used as per the terms of the Privacy Policy”
3. Send button



SUBMIT



Data Protection Policy

Should be adopted by the Board and noted in Board meeting minutes.

Elements:

- Cover indicating version number, review date, nature of any revisions, date effective from
- Purpose and scope of the policy,
- Key definitions
- Obligations of the company
- Data protection principles



Data Protection Policy

Elements con'd:

- Subject access requests and data subject rights
- Sharing data with third parties
- Photographs and video
- Organisational measures
- Transferring personal data outside of the EEA
- Data Breach Notification
- Policy Implementation



Data Protection Policy – Implications for HR

- How is data protection currently addressed in your Employee Handbook?
- Should a specific HR data protection policy be developed or the organisational policy be amended to better reflect staff?



Data Protection Policy – Implications for HR

Staff are required to comply with the policy. Inform staff as follows:

- If recording activity on CCTV, then signage will be posted in full view
- Use appropriate data protection notices at the point of data capture
- Not share Employee personal information for direct marketing purposes outside of the organisation
- Data Retention Periods: employment statutes 3 years; employment permits 5 years; parental leave 8 years; accident records 10 years



Data Protection Policy – Implications for HR

Inform staff as follows:

Employees expected to keep personal data secure:

- Desks and cupboards should be kept locked if they hold personal data
- Paper documents containing personal should be shredded
- Ensure that individual monitors do not show personal data to passers-by and that employees log off from their PC or password protect their PC when it is left unattended



Data Protection Policy – Implications for HR

Inform staff as follows:

Purposes for which staff records are held:

- Administration and management of the organisation
- Payment of salary and calculate benefits
- General human resources management
- Enabling organisation to comply with its legal obligations as an employer



Data Protection Policy – Implications for HR

Inform staff as follows:

Main categories of data held:

- Name, address, contact details, PPS number
- Details of approved absences (career breaks, maternity, parental leave, study leave, etc.)
- Details of work record
- Details of any accidents/injuries sustained on Organisation property or in connection with the staff member carrying out their duties
- Details of salary and other benefits



Data Protection Policy – Implications for HR

Inform staff as follows:

Main categories of data held:

- Personnel records including contract and offer letters, performance management information and, if applicable, records of any interactions under the headings of grievance and discipline
- Training courses completed and qualifications awarded
- Occupational health reports and sick certificates
- Records of application and appointment to promotion posts



Data Protection Policy – Implications for HR

Inform staff as follows:

Main categories of data held:

- CCTV data
- Email system data
- Financial data
- Human resources data
- Phone records



Data Protection Policy – Implications for HR

Inform staff as follows:

How data is obtained:

- Personal data is normally obtained directly from the Employee
- However, may be necessary to obtain data from third parties
e.g. references from previous employers



Data Protection Policy – Implications for HR

Inform staff as follows:

Opt-out: Organisation will cease processing the information unless it has a legitimate business interest that prevents this

Request erasure: Comply if there is no legitimate reason for the Organisation to keep it. Any third parties who process or use that data will comply with the request.



Data Protection Policy – Implications for HR

Inform staff as follows:

Storage:

- Ensure that only authorised personnel have access to an Employee's personnel file
- The Employee's Manager or Supervisor may have access to certain personal data where necessary



Data Protection Policy – Implications for HR

Inform staff as follows:

Storage:

- Ensure that only authorised personnel have access to an Employee's personnel file
- The Employee's Manager or Supervisor may have access to certain personal data where necessary



Data Protection Policy – Implications for HR

Inform staff as follows:

Changes in personal details:

- Employees are responsible for ensuring that they inform their Manager of any changes in their personal details e.g. change of address
- The company will need to keep personnel data for a period of time in order to protect its legitimate interests



Data Protection Policy – Implications for HR

Inform staff as follows:

Medical records:

- The Organisation reserves the right to carry out pre-Employment medicals as part of the recruitment process. This data will be retained by the Organisation.
- Request of medical records by employee subject to doctor's decision in accordance with Statutory Instrument No. 82 of 1989



Data Protection Policy – Implications for HR

Practical Question:

Are there circumstances in which a data breach is serious enough to be considered gross misconduct? If so, give examples.



Data Matrix – Demonstrating Compliance

Practical Question:

What fields of data does your data matrix/processing log contain? Can this document be developed into a reference guide for staff and volunteers?

- Review Data Matrix template



Data Protection Framework – Policy and Procedural Documents

Framework documents:

- Data Protection Policy
- Privacy Policy/Statement
- Data Matrix/Processing Log
- Information Security Policy
- Bring Your Own Device Policy
- Remote Access Policy



Data Protection Framework – Policy and Procedural Documents

Framework documents:

- I.T., Telecommunications, Email and Internet Policy
- CCTV Policy (if applicable)
- Data Retention and Erasure Policy
- Data Breach Policy and Procedures
- Subject Access Request Procedures
- Data Processor Agreements (MailChimp Sample)
- Access Control and Asset Management Policies



Data Protection Framework – Policy and Procedural Documents

Framework documents:

- Clear Desk and Safe Disposal Policies
- Risk Management Policy/Risk Register

Data Protection Framework – Policy and Procedural Documents

Practical Question:

Can some policies be incorporated into a single overarching policy document e.g. information security policy?

- IT Assets; Access Control; Password Control; Email; Internet; Antivirus; Information Classification; Remote Access; Outsourcing; Clear Desk; Redacting; Retention & Disposal; Cloud Storage; Data Backup; Cyber Security



Data Protection – Systematic Monitoring

What methods will you use to ensure that data protection policies are being adhered to within the organisation?

Do you need to develop a Data Protection Risk Register?

Are there implications for your organisation's risk register?

Data Protection – Systematic Monitoring

Examples of Risks:

- Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by “hackers”.
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.

Data Protection – Systematic Monitoring

Examples of Risks:

- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.



Data Protection – Systematic Monitoring

Examples of Risks:

- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.

Data Protection – Systematic Monitoring

Examples of Risks:

- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Data Protection – Systematic Monitoring

Examples of Corporate Risks:

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
- Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of your organisation's use of personal information may lead to a reluctance on the part of individuals to deal with your organisation.

Data Protection – Systematic Monitoring

Examples of Corporate Risks:

- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your company keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against your organisation. Under the GDPR you may also be liable for non-material damage.



Data Protection – Systematic Monitoring

Suggested data protection solutions to handle risks:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.

Data Protection – Systematic Monitoring

Suggested data protection solutions to handle risks:

- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.

Data Protection – Systematic Monitoring

Suggested data protection solutions to handle risks:

- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have with your organisation.
- If you are using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

Complying with GDPR Requirements

What actions do you need to prioritise next?

