General Data Protection Regulation

September 2018

Facilitator: Caroline Egan, CramdenTECH Ltd.

CramdenTECH

Topics

- The GDPR in Context
- Data Protection Principles
- Rights of Individuals
- Obtaining Consent
- Privacy Notices
- Data Security
- Data Breaches
- Preparing for the GDPR and demonstrating compliance

The GDPR & Data Protection Act 2018– Quick Overview

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

The GDPR in Context

- It heightens accountability for how personal data is acquired and handled
- It gives EU residents more control over their personal data
- It applies to sole traders and organisations established in the EU/EEA and to those outside of the EU that process the personal data of EU residents (including cloud computing service providers).

The GDPR – who does it apply to?

- Organisations who collect, share and use the personal data of EU/EEA residents

- Organisations who offer goods and services to, or monitors EU residents, then the GDPR applies, irrespective of the country where the organisation is established. Thus, the GDPR has expanded the territorial scope of EU data protection law.

The GDPR - Terminology

Personal Data

Any information relating to an identified or identifiable natural person. Examples of personal data include a person's name, home address, photo, an email address, bank details, posts on social networking sites and medical records.

The GDPR - Terminology

Sensitive Personal Data

The GDPR applies to sensitive personal data, which it refers to as "special categories of personal data". These special categories of sensitive data include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, genetic data and biometric data.

Processing

Applies to both automated personal data and to manual filing systems where personal information is accessible according to specific criteria.

The GDPR - Terminology

Data Controller

- A data controller is a person, organisation, company or legal entity who controls and is responsible for keeping and the use of personal data on computer or in structured manual files. Examples of data controllers would be pharmacists and General Practitioners.

Data Processor

- A data processor is a person, organisation, company or legal entity who processes personal data, but does not exercise responsibility for or control the personal data. Examples of data processors would include payroll companies, market research companies and accountants.

GDPR – Clarify Processing Activity

- **Commercial/operational activity**: examples of types of processing you conduct
- **Recruitment**: how people apply for jobs, online, email, snail mail
- **Employment**: paying salaries, attendance record, PAYE, paying expenses, personnel files, appraisals, grievances
- **Workplace**: CCTV, accident reporting, issuing security cards
- **Communications**: signing up for newsletters & direct mail

Anything else? List the types of personal data in your organisation.

Data Journey – Map

- All points of contact with the data subject where personal data is captured or recorded
- All staff members and third parties who have access to data subjects's personal data at any stage
- All locations (both digital and physical) where personal data is stored
- Methods and procedures used to safeguard personal data during collection, processing, storage and deletion

Practical Exercise

- Can you identify the ‘data journey’ in your organisation? What are the steps or stages in the journey?

- What are the implications of the data journey from a data processing, cyber security and human error perspective?

GDPR - Five Key Steps to Data Safety

1. **Identify the data you process and store**

- What Personal Data do you collect and process?
- Is the data accessible without the consent of the data subject? (how did you get the data)
- Is the data forwarded to a third party? If so, make sure that agreements with them identify them as data processors.
- If data processors are outside of the EEA, you may need an additional contract to enable you to send the data to the country or supplier.

GDPR - Five Key Steps to Data Safety

2. Create your data purpose(s)

- If you already have a stated data purpose, then make sure it is up-to-date i.e.:
    - . What data is collected
    - . Why it is collected
    - . How it is processed, by whom and where (within/outside EEA)
    - . How long it will be retained for
    - . Who to contact in case of a data protection query

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing …

- There must be a lawful basis for processing personal data.

- Processing may take place on the basis that the data subject has consented to such processing.

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing …

- Processing may take place on the basis that it is necessary to enter into or perform a contract with a data subject.

- Processing may take place on the basis that the data controller has a legal obligation to process the data.

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing …

- Processing may take place on the basis that it is necessary to protect the “vital interests” of the data subject.

- Processing may take place on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing …

- Processing may take place on the basis that the data controller has a legitimate interest in processing the data as long as the rights and freedoms of the data subject does not override this legitimate interest.
- Where a legitimate interest is the basis for processing, clear records of the organisation's assessment of the legitimate interest should be maintained and details provided of how the interests of data subjects have been considered.

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing, further points to note …

- Individual member states may introduce additional lawful grounds for limited processing connected with national law or the performance of tasks in the public interest.
- Personal data relating to criminal offences should be treated as Sensitive Personal Data for processing purposes. However, the criminal laws of individual member states are not governed by the GDPR.

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing sensitive personal data. Conditions to be met:

- Explicit consent
- Employment law
- Vital interests
- Charity or Not-For-Profit Bodies
- Data made public by the data subject

GDPR Implications - Five Key Steps to Data Safety

2. Create your data purpose(s)

Grounds for processing sensitive personal data. Conditions to be met:

- Legal claims
- Reasons of substantial public interest
- Medical diagnosis and treatment
- Public health
- Historical, statistical or scientific purposes
- Exemptions under national law

GDPR - Five Key Steps to Data Safety

3. Ensure Consent

- Make sure you are obtaining the Data Subject's consent to use their personal data
- Record their consent(s). Be able to demonstrate consent to the Data Subject or the Data Protection Commissioner (Subject Access Request or complaint)
- Where existing data has no record of consent for it, you may want to look at actively re-establishing consent. In some cases (such as in the provision of an active service) consent may be implied, but this point should be considered.

GDPR - Five Key Steps to Data Safety

3. Ensure Consent

- Make sure you are obtaining the Data Subject's consent to use their personal data
- Record their consent(s). Be able to demonstrate consent to the Data Subject or the Data Protection Commissioner (Subject Access Request or complaint)
- Where existing data has no record of consent for it, you may want to look at actively re-establishing consent. In some cases (such as in the provision of an active service) consent may be implied, but this point should be considered.

GDPR - Five Key Steps to Data Safety

4. Support the data subjects' rights

- Check that your internal processes, procedures and computer systems are able to support a Data Subject's rights within the time frames dictated by the GDPR.

GDPR - Five Key Steps to Data Safety

5. Create an incident response plan

- If a data breach occurs, ensure that an Incident Response Plan is in place to guide the process that will enable the correct response to be made.

    Following the discovery of a data breach incident involving personal data the Data Protection Commissioner or the Data Subject will be informed as to the nature and scale of the breach, the action that has been taken, the potential impact on the Data Subjects, and all within 72 hours of the discovery of the breach!

Methods of Demonstrating Compliance

Documentation

Organisations should maintain relevant documentation concerning its data processing activities. Organisations must record the following information:

- Name and details of the organisation. Where applicable the name(s) and detail(s) of other data controllers, data protection officer and representative(s) should also be recorded.
- Purposes of the data processing.
- Description of the categories of individuals and categories of personal data being processed.
- Categories of recipients of personal data.
- Details of transfers to third countries and clear documentation of the mechanisms in place to safeguard data transfer.
- Data retention schedules.
- Description of technical and organisational security measures.

Methods of Demonstrating Compliance

Technical and Organisational Measures

- Organisations should review and update data protection policies as necessary, train staff (and volunteers), address human resources implications of the GDPR and conduct an audit of data processing activities, with a view to amending and updating data processing activities.

Data Protection by Design

- In developing data processes, organisations should design implementation of the principles into data processes early on, particularly with respect to data minimisation, transparency, pseudonymisation, storage limitation, security features and the ability of individuals to monitor data processing.

Methods of Demonstrating Compliance

Data Protection by Default

Organisations should ensure that default service settings are data protection friendly for individuals.

Data Protection Officer

Where appropriate, appoint a Data Protection Officer (DPO). A DPO must be appointed if an organisation is:

- A public authority (except for courts acting in their judicial capacity)
- carrying out large scale systematic monitoring of individuals e.g. online behaviour tracking
- carrying out large scale processing of special categories of data or data relating to criminal convictions and offences

Methods of Demonstrating Compliance

DPIA

- Where appropriate, carry out data protection impact assessments. Organisations must carry out a DPIA when using new technologies and data processing is likely to result in a high risk to the rights and freedoms of individuals.

Code of Conduct

- Where available and appropriate, adhere to appropriate codes of conduct or certification.

Penalties for non-compliance with the GDPR

- Fines of up to €20,000,000 (or 4% of total annual worldwide turnover, whichever is greater)
- GDPR makes it easier for individuals to bring private claims against data controllers when their data privacy has been infringed or breached.
- The GDPR also allows data subjects who have suffered non-material damage as a result of a breach or infringement, to sue for compensation.

Data Breaches

- The GDPR requires that certain data breaches be reported to the relevant supervisory authority. A personal data breach refers to a breach of security that leads to the destruction, loss, alteration, unauthorised access to, or unauthorised disclosure of personal data.

- The relevant supervisory authority must be notified when the breach is likely to result in a risk to the rights and freedoms of individuals. In cases where data breach risks to individuals are deemed to be ‘high’, the individuals concerned must also be notified.

Data Breaches

- The relevant supervisory authority must be notified within 72 hours of the organisation becoming aware of the breach. If a data breach is so serious that the public must be informed, the organisation must do so without undue delay.

- Fines are significant (up to €10 million or 2% of worldwide annual turnover) for failure to notify a data breach when required to do so.

Data Cyber Security - What to Audit?

Standard Policies such as:

- Privacy Policy
- Information Security Policy
- Network Security Policy
- BYOD Policy
- Remote Access Policy
- Information Technology, Telecommunications, Email and Internet Policy

What to Audit?

- **I.T. Personnel**

  Who is responsible for implementing data and cyber security in the company? What level of training have they received in the last two years of relevance to their roles?

- **I.T. Strategic Development Plan**

  Does the company have an I.T. Strategic Development Plan?

- **Cyber Security Operational Plan**

  Does the company have a Cyber Security Operational Plan?

What to Audit?

- **Asset Management**

  Is an up-to-date asset management policy in place?

- **Wireless Networks**

  Are wireless networks appropriately secured?

- **Operating Systems**

  Are operating systems and software efficacy reviewed on a scheduled basis?

What to Audit?

- **Filtering Software**

  Is email and internet traffic filtering software in place?

- **Servers**

  Is a list of servers available and the names of the people who are responsible for checking that servers are up-to-date?

- **Firewalls**

  Are appropriate firewalls and intrusion detection software in place?

- **Configuration Management**

  Is appropriate configuration management in place?

What to Audit?

- **Security Scans**

  Are security scans reviewed on a scheduled basis?

- **Anti-virus Software**

  Is anti-virus software loaded onto all devices in use in the company and active at all times?

- **Backups**

  Are data backups made on a scheduled and regular basis? Are data backups encrypted?

- **Log Files**

  Are log files maintained for at least 12 months? Are automated analytics used on log files?

What to Audit?

- **File Transfer**

  Are appropriate security mechanisms in place for transferring and sending files?

- **Hardware Inventory**

  Is a hardware inventory list available and up-to-date?

- **Software Inventory**

  Is a software inventory list available and up-to-date?

- **USB Drives**

  Is a policy in place in the company concerning the use of USB drives by staff?

What to Audit?

- **Portable Devices**

  Is a policy in place in the company concerning the use off-site of portable devices such as laptops?

- **Data Classification**

  Is data classified by risk and sensitivity?

- **Access Limits**

  Does the company limit access to data appropriately?

- **Encryption**

  Is the encryption of data at rest and encryption of data in transfer adequate?

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.

Consent

- The GDPR requires that individual consent must be freely given, informed, specific and clearly indicate an individual's wishes.
- Consent has to be verifiable.
- Organisations processing data based on individual consent, must ensure that individuals 'opt-in' and can easily withdraw consent.
- In preparation for the GDPR, it may be necessary for some organisations to seek consent from individuals afresh – in they feel that existing consent mechanisms do not stand up to GDPR requirements.

Consent and Children

- The GDPR enhances the protection of children's personal data. Where services are offered directly to a child, an organisation must ensure that its privacy notice in a very clear and plain way i.e. in a way that the child will understand.
- If an organisation offers online services to children, it may need the consent of a parent or guardian to process personal data relating to a child. Parental/guardian consent is not required when data processing is related to preventative or counselling services offered directly to a child.

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.

Privacy - The Individuals Right to Information

Most organisations will need to update their privacy statements. Some excellent resources to help with this task:

- https://www.econsultancy.com/blog/69256-gdpr-how-to-create-best-practice-privacy-notices-with-examples

- https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

Privacy - The Individuals Right to Information

- Identity and contact details of the data controller and where applicable the controller's representative
- Identity and contact details of the Data Protection Officer (if one is appointed)
- Purpose of the data processing
- The lawful basis for the data processing
- The legitimate interests of the data controller or third party (if applicable)

Privacy - The Individuals Right to Information

- Any recipient or categories of recipient of the personal data
- Details of data transfers to third countries and data safeguards
- Data retention period or criteria used to determine the retention period
- The existence of each of the data subject’s rights
- The right to withdraw consent at any time (where relevant)

Privacy - The Individuals Right to Information

- The right to lodge a complaint with a Supervisory Authority

- Whether provision of the personal data forms part of a contractual requirement or statutory obligation and consequences of failing to provide the data

- The existence of automated decision making (including profiling) and information about how decisions are made, significance and consequences

Data Subject Policies and Procedures

Data controllers should ensure that they have adequate policies and procedures in place to enable them to uphold the rights of data subjects. Organisations should consider questions such as:

- Is there a documented policy/procedure for handing subject access requests?
- Are individuals provided with a means to request access to data held about them?
- Can the organisation respond to a subject access request within one month of receipt of a request?

Data Subject Policies and Procedures

- Can data subjects get their personal data in a structured, commonly used and machine readable format?
- Are data subjects informed of their right to demand rectification or erasure of personal data held about them (where applicable)?
- Are there controls or procedures in place to enable personal data to be erased or restricted?

Data Subject Policies and Procedures

- Are data subjects told about their right to object to certain types of personal data processing?
- Is profiling based on the explicit consent?
- Does any profiling use sensitive personal data?
- Does any profiling use children’s data?

The GDPR – Staff Awareness

- Use a Staff Awareness Checklist to help identify GDPR staff training requirements and action areas.

The GDPR – Staff Awareness

- Familiarise yourself with the organisation's data protection policy.
- Follow the organisation's security protocols for obtaining, handling, sharing and using personal data.
- Ensure that all smart devices and computer equipment have secure passwords.
- Encrypt sensitive and confidential information stored on smart devices and computer equipment.
- When using the organisations smart devices or computer equipment away from your office, ensure that no other person (or CCTV) can view your work screen.

The GDPR – Staff Awareness

- When working away from the office, lock your organisation smart devices and computer equipment in the boot of your car, where possible.
- Unless you can do so securely and it is absolutely necessary for work purposes, do not take USB or portable storage devices containing personal data, sensitive or confidential data out of the office.
- Do not read organisation-related hard copy documents and files containing personal data, sensitive or confidential information in a public place where they can be overseen by others or CCTV.

The GDPR – Staff Awareness

- Always check a meeting room or meeting place for organisation-related hard copy documents and files before you leave a meeting location. Don’t risk leaving documents behind!
- Check hard copy documents before discarding them in rubbish bins. Follow the organisation policy for shredding sensitive or confidential information.
- In the office, keep hard copy personal data and sensitive and confidential information securely locked away in a filing cabinet.
- Clear your desk. Do not keep personal data, sensitive or confidential information in your in-tray or visible to others on your desk.

The GDPR – Keeping Data Secure

- Check an email before you click ‘Send’ and ‘Reply All’. Is there sensitive or confidential information contained in the email or attachments, including in previous emails in a chain of correspondence?
- Check social media posts before uploading or commenting. If you post sensitive or confidential data online, you may have no control over who views the information.

The GDPR – Remember?

Data Review

- Review the data your organisation holds, where the data came from, for how long it has been held and the legal basis for processing data.

Review Privacy Information

- Review the organisation's privacy notices and amend where necessary.

The GDPR – Remember?

Individuals' Rights

- Ensure that individuals' rights are safeguarded in any procedures or processes used in or by the organisation.

Data Subject Access Requests

- Review and update where necessary policies and procedures to deal with data subject access requests and ensure that requests can be complied with within a 30 day period.

The GDPR – Remember?

Lawful Basis for Processing

- Review the legal basis for processing personal data in your organisation to ensure that it is still relevant and GDPR compliant.

Consent

- Review the organisation's methods for obtaining consent and ensure that they are GDPR compliant.

Children

- If your organisation offers online services to children, ensure processes and mechanisms are in place to verify the age of children and to seek parental consent where necessary.

The GDPR – Remember?

Data Breaches

- Ensure that procedures are in place that will enable the organisation to notify the Supervisory Authority within 72 hours if a data breach occurs and data subjects if required.

Data Protection Impact Assessments

- If the organisation engages in data processing likely to result in high risk to individuals, carry out data protection impact assessments.

The GDPR – Remember?

Data Protection Officers

- Assess whether or not your organisation needs to appoint a Data Protection Officer.

International Data Transfer

- If your organisation operates in more than one EU/EEA country, identify the Supervisory Authority in each country in which you operate.

Review

- What are the next steps for your organisation? What further actions do you need to take to comply with the GDPR?

- Facilitator: Caroline Egan, CramdenTECH Ltd.

caroline@cramdentechsolutions.com

www.buildfutureskills.com