GDPR Part 1: Understanding the Legal Framework and Key Legal Requirements

What is the GDPR?

- This puts in place the GDPR within the UK legislation.
- Adopted within the UK after Brexit
- Minor adjustment post Brexit
- Have all had time to embed some principles and requirements – some more so than others.
- Sits alongside the:
    - **Data Protection Act 2018 (DPA)**
    - **Privacy and Electronic Communications Regulations 2003 (PECR) additional** restrictions on direct marketing by electronic means (phone, fax, email, text, video messaging), rules on cookies etc.
    - **Regulation of Investigatory Powers Act 2000 (RIPA)** covers 'interception' of communications (e.g. monitoring employee emails or internet usage, Instant Messenger etc.)

Why do we need GDPR?

- Clarify **consistent approach across members states in EU**
- **Enhanced rights for our personal data** to prevent misuse and abuse
- **Technology moved on** from the 90's – more sophisticated systems & more sophisticated use of technology;
- **More data online**, people share more personal information;
- **Protection:** Breaches / hacks of personal / sensitive info;
- **Tighten up DPA:** address many of the shortcomings in the DPA
- e.g. accountability and transparency, definitions, expanded rights to individuals

Who does it apply to?

- Applies to **any legal person or organisation that processes personal data**
- **Location:** orgs established in EU or processing personal data from EU.
- **All sectors:** voluntary, private, public, commercial.
- **Data controllers:** determines the purposes and means of processing personal data i.e. **YOU!**
- **Data processors** – person or body which processes data on behalf of a data controller e.g. payroll bureaux, database, third party mailing list client

- **GDPR places further obligations on Controller to ensure its contracts with processors comply with the GDPR**
- **GDPR, generally, does not apply to Business-to-Business communications (**PECR will apply until replaced by e-Privacy regulation). However, there may be elements of personal information contained within your business-to-business communications.

Main Implications

- Any **PERSONAL** Information collected, stored, processed.
- **Fundraising** – mainly direct marketing.
- **Employees & HR data** – individual rights apply.
- **Finance** – payroll & pensions, especially if using third parties e.g. payroll processor or sending auto-enrolment data to pension provider.
- **Marketing** – electronic / direct
- **Accountability:** understanding what you are doing with data and how you are protecting it.
- **Balancing** your need for data against the rights of individuals.
- Personal data available in the public domain is still personal data and Data Protection still applies to it.

Key Definitions

- **Data subjects** – any living, identifiable individual about whom personal data is processed, includes:
    - employees, contractors, consultants
    - volunteers, trustees
    - suppliers, customers
    - individuals on contact lists, e.g. fundraising/marketing databases
- **Personal data – any information relating to a living person who is identified (or can be identified directly /indirectly) from that information**
    - e.g. names, addresses, telephone numbers, job titles, date of birth, salary, county of origin, reason for coming here
      contained in a filing system – electronic AND manual (e.g. personnel files, online HR records, card indexes)
    - What other information might be within your records that doesn't fit into the main categories e.g. email, tel. could be health, legal, financial data etc. that may indirectly or directly identify that individual.
- **GDPR definition** also includes location data, genetic or biometric information (e.g. fingerprints), pseudonymised data – e.g. key-coded, unique reference numbers, IP addresses

Special Categories:

- **Requires higher level of protection** as the personal data is considered far more sensitive
    - e.g. Race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data (where used for identification purposes), health data, sex life, sexual orientation.
- **Criminal convictions and offences** dealt with separately in domestic legislation (Data Protection Bill)

Processing

- **Means anything done with personal data**
  - collection, recording, storing
  - organising, structuring
  - Altering
  - using, disclosing
  - erasing, destroying
  - GDPR definition – "whether or not by automated means", e.g. staff swipe card clock-in and clock-out system

Key Roles

Data Controller

- **Data controllers:** determines the purposes and means of processing personal data i.e. **YOU!** e.g. collecting bank details, address, contact info etc. YOU are the controller.
- If you work with others and have a relationship to share data than you need to understand the role you play.
- If you are a data controller you must determine the purposes and means of processing data.
- If you decide what you do with personal data, how you use it, collect it, etc. you are likely to be a data controller.
- Nobody tells you what to do with it or how to process it, it's your decision.
- In the context of fundraising and reporting to funders, you are still the data controller and decide what information is passed over to the funder to report on services and projects.

Data Processor

- **Data processors** – person or body which processes data on behalf of a data controller e.g. payroll bureaux, database, third party mailing list client
- **On behalf of is the key phrase**
- Am I using this information on behalf of another organisation?
- There may be complex arrangements between your organisation and it can be complicated to determine who has which role, but it is critical to determine this to understand your responsibilities and get this right from the beginning
- If you are storing the data you need to ask why. Am I storing it on behalf of someone else, or am I storing it for my own use
- SharePoint, Google etc. would be a data processor as they are storing your documents on behalf of your organisation.

Data Protection Officer vs Data Protection Duties

- Requirement for some organisations to appoint a **Data Protection Officer (DPO).**
- It is a requirement if you process large volumes of special category data.
- This is needed for large scale operations where a high volume of processing takes place.
- 'Large-scale' is not defined in the legislation and can vary from organisation and context of their work. What is the actual activity of the organisation?
- If you don't need a DPO, you should still ensure that GDPR is assigned to a role within the company and is part of someone's job description.
- **You must be able to demonstrate that these responsibilities are covered by someone.**

Information Commissioners Office (ICO)

- The regulatory body in the UK For data protection.
- Involved with non-compliance
- Uphold information rights in the public interest
- Monitor application and compliance of UK GDPR
- **Investigative powers**, including:
    - Order controller and processor to provide information
    - Data protection audits
    - Entry, inspection and seizure (documents and equipment)
- **Corrective powers**, including:
    - Warnings, reprimands and orders for compliance
    - Temporary or definitive ban on processing
    - Order the rectification or erasure of personal data or restriction of processing

Key ICO Concepts

- ICO expects "comprehensive but proportionate governance measures"
- Privacy by design and default (e.g. data minimisation, pseudonymisation, creating and improving security features on an ongoing basis)
- **Appropriate technical and organisational measures**
    - data protection policies and reviews of existing policies
    - staff training (on induction and every 2 years)
    - internal audits of processing activities
- **Documentation -** requirement to keep records of processing activities
- Requirement for some organisations to appoint a **Data Protection Officer (DPO)**
- Compulsory **Data Protection Impact Assessment (DPIA)** for **high risk processing (privacy by design)**

Penalties

- Old DPA didn't really have many penalties
- **New DPA has much bigger fines** of which there are two levels:
    - Fines of 10 million EUROS or up to 2 % of annual worldwide turnover, whichever is higher OR 20 million EUROS or up to 4 % of annual worldwide turnover, whichever is higher
- When deciding on whether to impose a fine, ICO will consider:
    - Nature and gravity of infringement
    - Purpose of processing concerned
    - Number of data subjects affected
    - Damage or potential damage suffered by them.
- Fines are more of concern within private sector as there is a real sense or possibility of data breach
- ICO wants to help organisations to better understand how they can better comply and keep service users secure and safe.

Data Protection Principles

1. **Lawfulness, fairness and transparency –**
    a. **Lawfulness** - before you process information, make sure you know what your legal basis is!
    b. **Fairness** - you must make sure you are not using data for unreasonable purposes
    c. **Transparency** - Be open about that you are using it for, how you are sharing it and how it is being used. People have a right to know what you are doing with their information.
2. **Purpose Limitation**
    a. Lots of people have a database full of people's details.
    b. The purpose for what you collect the data has to be the purpose for what the data was collected. You can't just email all your contacts on the database if they didn't provide the information for this activity e.g. asking for donations when they only consented to receive your newsletter.
3. **Data minimisation**
    a. Do not collect more than you really need for the purpose
    b. Keep this as basic as possible for personal data
4. **Accurate and up-to-date**
    a. The ICO says it is up to the user to let us know if data has changed.
    b. You should promote that you are open to keeping data up-to-date
    c. You should make every reasonable effort to keep this updated
    d. Have a process in place to show this is up-to-date
    e. E.g. if the user is inactive for 12 months, send out an email or get them to update details or confirm nothing has changed.
    f. Be mindful, check processes, have processes for checking and keeping data updated.
    g. Ensure that personal data can be **rectified** or **erased** without delay.

5. **Storge Limitation**
    a. Do not store personal data for longer is required.
    b. If you don't need it any longer get rid of it.
    c. Must have a retention schedule for different types of data e.g. employee data, how long do you keep this?
    d. Bear in mind statutory regulations e.g. financial record keeping.
    e. If you are the processor, the processor should ask the controller how long they should keep the information for.
    f. Controller has an obligation to inform the processor how long to keep the data on their behalf.
6. **Integration and Confidentiality (security)**
    a. Technical and organisational measures to keep data up-to-date
    b. Especially where you are sending data outside of the system.
    c. Office 365 has some protections to help safeguard sensitive or

d. processed in a manner that ensures **appropriate security** of the data (including to prevent unauthorised or unlawful processing, accidental loss, destruction or damage) using appropriate **technical or organisational measures**
e. must **not be transferred outside the EEA** unless the country has an adequate level of protection for data subjects or appropriate safeguards are put in place (e.g. USA)

7. **Accountability**
    a. Must be able to demonstrate compliance with the data protection principles.
    b. You have a privacy notice, we only keep data for the purposes it was collected.

Lawful Basis for processing

1. **Consent**
2. **Contract**
3. **Legal obligation**
4. **Vital interest**
5. **Public task**
6. **Legitimate interest**

Consent

- **freely given, specific, informed** and **unambiguous** indication of the data subject's wishes by a **statement** or by a **clear affirmative action** if verbal – whatever is appropriate for the activity you are collecting personal data for.
    - **Freely given** - Did you give this freely or as a condition for something else? It can't be tied to any condition.
    - **Specific** – I will consent for this specific purpose. I ticked the box to receive email, NOT SMS.
    - **Informed and unambiguous** – why do you want this, what will you use it for? Has to be clear and informed.
    - **Clear affirmative action** – forms being used to collect consent which is a statement without any mark to show that they are actively affirming this

- Should signify agreement to the processing of personal data relating to the individual i.e. best practice signing or written note of consent
- Verifiable – **keep records** of how and when given
- Children –under 13 in UK – seek parental/guardian consent

Valid consent

- A positive opt in – don't use pre-ticked boxes or default consent.
- Need to be able to have the choice to opt in
- Requires a very clear and specific statement of consent.
- Make it easy to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told them.
- If you take consent over the phone then this needs to be documented in a record.
- - must be in an **intelligible** and **easily accessible** form
  - must use **clear** and **unambiguous** language
  - if written document contains other matters (e.g. contract of employment), the request must be **clearly distinguishable from other matters**

- Individual has the **right to withdraw consent** at any time and should be informed of this right before giving consent (this needs to be flagged)

Children and Consent

- Extra layers of consent for children.
- Required for children under 13 years.

Contract

- Have a direct contract with the person who's personal data you might be processing e.g. payroll services, employee contract

Legal Obligation

- Trying to fulfil a legal requirement of the organisation itself or third party e.g. HMRC requesting tax information.

Vital Interest

- Where you need to act in the best interest of the individual.
- Usually for the life and death scenario
- e.g. passing on medical or personal issue in an emergency.

Public Task

- to carry out a public duty e.g. local authority, NHS, police etc.
- they are processing personal information as part of their public duty

Legitimate Interest

- Not very popular anymore.
- Can't be used by public sector
- In order to use legitimate interest you have to do a **legitimate interest check** to make sure this doesn't override the individuals rights:
    - **Purpose Test**: are you pursuing a legitimate interest?
    - **Necessity Test**: is the processing necessary for that purpose?
    - **Balancing Test:** do the individual's interests override the legitimate interest?
- If DPIA indicated your need for data overrides the rights of the individual then you need to pick another legal basis.
- Legitimate interest should be the last resort as it is very difficult to balance the interest of the organisation of the rights of the interest. The individual's rights are nearly always more important.
- Need to look at processing activity you are trying to achieve.

Special Categories of Personal Data

If you process special category data you must first identify the legal basis (Article 6), then you must also substantiate that with one of the following conditions:

1. **Explicit consent** (opt-in)
2. necessary for carrying out **obligations under employment, social security** or **social protection** law, or a collective agreement

3. necessary **to protect the vital interests** of the data subject
4. **provision of health or social care or treatment** or management of health or social care systems and services or a contract with a health professional / **administering justice / statutory functions**
5. Data made public by data subject
6. Archiving and researching in the public interest.

Therefore, for the majority of charities collecting special category data, the likely category here would be **explicit consent.**

Data Subjects' Rights

Most Rights have a window of 1 month to respond to.

Right to be Informed

- If you want to have my information then I have a right to know why you want it, what you are going to do with it, where the data is held and how long you will keep it for.
- To comply, you must be able to ascertain whether you have answered those questions for the person providing the data.

Right of Access

- If you have my information then I have a right to see what data you have on me.
- If the data is sat in an archive, it's still being processed because its being stored.
- Increase in Subject Access Requests
- Must provide copy of information **free of charge** – can charge 'reasonable fee' if request manifestly unfounded or excessive
- **1 month** (at the latest) to comply – can be extended where requests are complex or numerous
- If request made electronically, provide information in a commonly used **electronic format**

Right of Rectification

- The right to have wrong information corrected if **inaccurate** or **incomplete**
- Respond within **1 month** –can be extended where request is complex
- If data disclosed to third parties, must also inform them of the rectification where possible

Right of Erasure (to be forgotten)

- If requested, the person can ask for all their data to be deleted, except where you have a legal reason to keep any of the information.
- This needs to go just beyond a mailing list – there may be other records where the person's information crop up.
- You can use tools like MS office to help you identify and locate files, emails and documents.

Right to Restrict Processing

- Can keep the data but no longer process any activity relating to that individual, until any query regarding processing is cleared up

Right to Data Portability

- Right to take information with you and port it across to another system in an accessible format e.g. .csv. be mindful that this is data you have provided yourself.
- Must be provided **free of charge within 1 month**
- Allows individuals to obtain and reuse their personal data for their own purposes across different services
- Allows them to move, copy or transfer personal data easily from one IT provider to another. Must provide copy of information **free of charge** – can charge 'reasonable fee' if request manifestly unfounded or excessive
- **1 month** (at the latest) to comply – can be extended where requests are complex or numerous
- If request made electronically, provide information in a commonly used **electronic format**
- another in a safe and secure way, without hindrance to usability

Right to Object

- Individuals have the right to object to:
    - processing based on **legitimate interests** or performance of a task in the public interest/exercise of official authority
    - Direct marketing (including profiling)
    - Processing to purposes of scientific/historical research and statistics
    - **Legitimate interests** – stop processing **unless** compelling legitimate grounds or legal claims
- You cannot object if the information is being used to fulfil a legal purpose, you cannot object

Right to object to Automated Decision Making and Profiling (AI etc.)

- If Automated Decision Making and Profiling is used to process personal data to make decisions about you then you have a right to have a human look a this e.g. automated benefit appeals, recruitment opportunities etc.