Editors' Note: This document has been assembled for AAMET by Alan Robinson,

WHAT IS DATA PROTECTION?

LEGAL RULES that apply whenever we process data belonging to an individual who can be identified.

WHAT IS GDPR?

It is the **GENERAL DATA PROTECTION REGULATION.**

- Biggest overhaul of data protection since the Data Protection Act 1998.
- It is an EU Regulation and applies with direct effect to all EU member states.
- It amends existing rules on handling data to increase transparency, and accountability.
- It will apply IRRESPECTIVE OF BREXIT.

WHY DOES IT AFFECT VOLUNTARY ORGANISATIONS?

Data Protection legislation applies to all **data controllers.**

A **data controller** is

- A natural or legal person, public authority, agency or other body ….
- Who or which alone, or jointly with others …
- Determines the purposes and means of the processing of personal data.

Which means that …

- ANY organisation or group …
- That holds any kind of personal data, AND …
- Is responsible for deciding what happens to that information …

… is a data controller.

You need to **show** you understand the risks in processing other peoples' data. This means holding basic information to demonstrate this.

WHAT IS PERSONAL DATA?

It applies to all personal information concerning living individuals.

It identifies an individual:

- Susan Smith probably not
- Alan Robinson possibly, especially if e.g. linked with an email address.
- Sir Andy Murray definitely

It includes all people – staff, volunteers, clients or customers, beneficiaries, you …

It applies whatever you are doing with the data – collecting, using, deleting, anonymising and everything in between.

Some data is **SENSITIVE PERSONAL DATA**

This includes:-

- Racial/Ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- TU membership,
- Genetic/biometric for identification,
- Health,
- Sex life and sexual orientation.

Generally EXPLICIT CONSENT is needed to process sensitive data. It is sufficient if the data subject has put it in the public domain.

HOW CAN WE PROCESS PERSONAL DATA?

THE FIRST PRINCIPLE OF DATA PROCESSING
PROCESSING DATA HAS TO BE FAIR, TRANSPARENT AND LAWFUL

To be lawful it must meet a condition in Article 6.

Article 6 conditions

- **Consent** which is clear, demonstrable, freely given, easily withdrawable, and unambiguous.
- Data which is processed for the **purposes of a contract**.
- There is a **legal obligation** to hold the data.
- Processing the data is in a person's **vital interests** (safer not to rely on this).
- Processing the data is necessary in the **public interest** (safer not to rely on this).
- Processing the data is necessary for the **legitimate interests of the organisation**, and the interests of the individual are not thereby prejudiced.

Commonly we expect to have the data subject's consent. Can you meet the definition of consent? The subject has to opt in, not opt out. Old style consent may not be enough.

FAIR PROCESSING – AN EXAMPLE

The Community Centre wants to use a photograph and name of a child who participated in a recent event in their community newsletter.

THE FIRST DATA PROTECTION PRINCIPLE APPLIES.

Processing must be:-

- FAIR
- TRANSPARENT
- LAWFUL

Is it Fair?

Look at the circumstances when you obtained the information.

- It was a public event
- Was it clear why you were taking the photographs? Professional photographer or 'snap'?

What would be a reasonable use in those circumstances?

What is the connection between the use for which you collected the information, and the use to which you want to put it?

Is it Transparent?

- How obvious is this use?
- What have you told your visitors and users about what you intend doing with their information?
- What's in your privacy notice?
- What's in your ICO register entry (if you have one)?

Is it Lawful?

Can you meet a condition in Article 6?

- Do you have consent from the child for this? How old is the child? What about the parents? Can you get both to cover yourself?
- Or is it necessary for a task carried out in the public interest?
- Or necessary for the legitimate interests of the centre? What about prejudice to the individuals? If you take a photograph of the summer fun day at the Women's Refuge and send it to the press, it may seriously prejudice the interests of the subjects.
- Will it be making public information about the child? For example, if the centre is faith based, does it make public information about the child's religion?
- If so, is there explicit consent? Or is the information already in the public domain?

WHAT'S NEW IN GDPR?

- Requirement for certain policies
- Privacy Notices
- Data Protection Impact Assessments – new requirement for risky processing
- Data Processing Agreements – new requirements
- Individual rights (right to be forgotten, portability etc.)

PROOF IS KEY. Can you demonstrate that you have done all that you need to do?

WHAT DO YOU NEED TO DO NOW?

- Carry out a data audit. What data do you hold and why?
- Review the data you hold and consider whether you comply with the first principle.
- Prepare privacy notices and make available to all people whose data you hold.
- Do you need their consent? If so make sure you have it in writing. If you don't, you need either to delete the data or to decide which other Article 6 condition is applicable – and record it.
- Make sure you have all relevant policies in place
- If you have data processing agreements in place, review and amend.
- Ensure you have a procedure in place for people to exercise their individual rights.
- Ensure all your staff, volunteers, etc. know what has changed. Train your staff. Make sure you can demonstrate that you have done so.

PRIVACY NOTICES

If you collect data, you need to give a **PRIVACY NOTICE** to the people who are providing the data. This will include:-

- The identity and contact details of the Controller, and any Data Processor (see below);
- The purposes for which information is being collected;
- The legal basis for use of information:
    - If consent – mention that they can withdraw consent;
    - If necessary for legitimate interests – detail what those interests are;
    - If statutory requirement or contract – whether or not obligatory and consequences of not providing.
- Recipients/categories of recipients;
- Details of safeguards if outside European EA;
- Retention period or criteria used to determine the period;
- The existence of the rights to access information, rectification, erasure, object to processing, and data portability;
- The right to complain to the ICO.

POLICIES

YOU MUST HAVE policies that cover …

- What happens if there is a Data Breach. Need to tell the ICO within 72 hours, unless no breach to individuals. Need not tell individuals (but a good idea).
- Data Retention – how long data will be retained
- Use of sensitive information for employment
- Use of DBS information. This is what we hold; this is how we keep it safe.

A general data protection policy is optional, though it may contain all the necessary information to fulfil the policy requirement.

You may need a BYOD (bring your own device) policy. Whether you have a policy or not, YOU MUST CONSIDER WHETHER THIS APPLIES – the issue of staff and volunteers processing data on their own computers or phones.

DATA PROCESSORS

A third party acting under your instruction and control when doing something with personal data for you – for example, payroll providers.

You should already have a written agreement in place, but there are now additional requirements

Check IT contracts particularly

Add in:

- Duty of confidentiality on staff;
- Subcontract with Controller permission;
- Assist Controller with subject rights and security;
- Return or delete at end – controller's choice;
- Make info about activity available to controller.

INDIVIDUAL RIGHTS

- Subject Access – 30 days – no fee
- Rectification – right to have data corrected.
- Erasure – right to be forgotten
- Restriction – right to limit use of data to storage but not to process.
- Portability – retain and use personal data for own purposes across a range of settings.

DATA AUDITS

The first step is to **carry out a data audit.** By doing this, you will almost certainly be able to see what data you collect and what for, and what you need to do about it.

You need to know:

- What data you have,
- Where it is,
- Why you have it,
- How you got it,
- What you do with it,
- How long you need it.

Data Audit: What

Remember the definition of personal data

Identify what categories you hold as an organisation

- Employees/volunteers
- Members of the organisation
- Regular donors
- Contractors
- Any others?

What information do you hold about each category?

Data Audit: Where

Where do you keep your data?

PAPER

- Filing cabinets
- Home office
- Drawers
- Napkins … is that phone number on the Post It on the board personal data? It might be!

ELECTRONIC

- Databases
- Personal computers
- Memory sticks
- CDs
- Phones or laptops belonging to staff or volunteers?
- Floppy discs???

Data Audit: Why?

Why do you hold the data that you do?

This will depend on what it is

- Personal contact details for clients
- Communication about events
- Notices of meetings
- Payroll information
- Employee information
- Disciplinary record
- Prayer requests to a church
- Trustees and committee members contact details
- Baptism records for a church
- What else?

Data Audit: How do you collect data?

From the individual

From another person

- Friend
- Relative
- Statutory agency/body
- Previous advisers
- Previous church
- Social media …

Data Audit: What are you doing with the data?

Again – depends upon the information

- What **are** you using it for?
- What do you **want** to use it for?
- What **should** you be using it for?
- Are you transferring it to any third party?
    - Regularly
    - As a one off, occasionally
- Are there any "transfers" of electronic material to servers offsite? How is that data protected? You should be told by e.g. Googledocs.
- Do you use the Cloud? How is that protected?

Data Audit: How long do you need the data?

Are there any legal requirements e.g. minimum time to keep it?

If not …

- How long do you want it for?
- Can you justify that length of time?

If yes – that's how long you can keep it!

Data Audit: Apply the principles to your data.

Remember the First Principle: Processing shall be fair, transparent and lawful

What is reasonable? (FAIR)

What did you tell them when you obtained their information? (TRANSPARENT)

Can you meet an Article 6 Condition? (LAWFUL)

Article 6 conditions

- Clear, demonstrable, freely given, specific for each purpose required, easily withdrawable, unambiguous consent
- Purposes of contract
- Legal obligation
- Vital interests (e.g. next of kin details)
- Public interest
- Necessary for legitimate interests without prejudice.

And don't forget …

- Only use the data for the purpose for which it was obtained
- Only have what you need
- Keep everything accurate and up to date
- Keep it only as long as you need it
- Keep data safe. You decide what is safe. Need to assess risk and to show this has been done.
- Ensure individuals can access their rights
- Don't transport outside the European Economic Area without consent or safeguards.

AN EXAMPLE OF AN AUDIT TABLE FOR A VOLUNTARY ORGANISATION

WHO	WHAT	FAIR	TRANSPARENT	CONDITION
Trustees	Bank details Personal addresses Email addresses	Yes	See privacy policy	Consent Necessary for legitimate interest
Staff	Marital status/ sexual orientation[1]	Yes	See privacy policy	Legal Requirement? Consent? Legit interests? ???
Users	Photograph at church fete[2]	Maybe	Maybe. Previous examples?	Consent? Legit interests?
Volunteers	Home addresses Phone numbers Email addresses	Yes	See privacy policy	Consent Legit interests

[1] – may be unavoidable e.g. where employee uses title or from name of next of kin
[2] – see example above