Data Protection Factsheet

This factsheet covers the following key issues and topics relating to data protection for VCSE organisations:

- Data Protection Definitions
- GDPR Legislation
- Data Protection Policies and Procedures
- Resources and Support

Data Protection Definitions

Data protection is about keeping people's data safe and using it in a fair, transparent and responsible manner.

Personal data is legally defined in the UK as 'any information relating to an identified or identifiable person' and includes information that could lead to anyone being identified, either directly or indirectly. This is often data such as personal contact details and includes information you collect and that given to you by others.

The law also defines some sensitive personal data as **special category data | ICO** needing more protection. This includes information revealing racial or ethnic origin, political opinions, religious / philosophical beliefs or trade union membership; genetic, biometric or health data; and data concerning a person's sex life or sexual orientation. Separate rules and guidance apply for personal data about criminal offences.

The **Information Commissioner's Office** (ICO) regulates data protection in the UK and provides advice and guidance, considers complaints, monitors compliance and takes enforcement action where appropriate.

GDPR Legislation

Data protection legislation relates to all those about whom you keep personal data other than for your own family/household purposes: your members, workers, volunteers and service users. It regulates how organisations collect, store and use personal data and ensures this is done responsibly and transparently.

People have legal individual rights | ICO to know what data you have about them and how it is used, see that information and correct it if necessary, and ask for it to be erased or limited in how it is used.

The **Data Protection Act (DPA) 2018** replaced the Data Protection Act 1998 and was amended on 1 January 2021 by the **UK General Data Protection Regulation (GDPR)** under the European Union (Withdrawal) Act 2018. The UK GDPR is based on the EU GDPR, which applied in the UK before 2021, but with some changes for a UK context.

The DPA 2018 and the UK GDPR complement each other: the key principles, rights and duties for processing of most personal data in the UK are set out in the GDPR and separate rules for law enforcement, national

security and defence together with the Information Commissioner's role are outlined in the DPA. For most organisations, part 2 (the general processing regime) of the DPA 2018 will apply alongside the UK GDPR. The ICO has developed a detailed Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

The GDPR outlines seven **key principles** which should form the basis of your approach to handling personal data:

- Lawfulness, fairness and transparency (tell people what you will do with their data)
- Purpose limitation (only use people's data for what they have agreed)
- Data minimisation (don't keep data you don't need/use)
- Accuracy (make sure data is correct and up to date as far as possible)
- Storage limitation (don't keep data after you have finished using it)
- Integrity and confidentiality (take reasonable measures to keep your data secure)
- Accountability (keep records to show you have complied with the principles)

It also sets out the **lawful basis** for processing personal data, of which at least one must apply:

- Consent (from the individual for a specific purpose)
- Contract (to fulfil a contract with the individual)
- Legal obligation (to comply with the law)
- Vital interests (to protect someone's life)
- Public task (to perform a task in the public interest or for your legal role)
- Legitimate interests (for your legitimate interests or those of a third party)

Your lawful basis for processing | ICO must be determined and recorded before you start to process personal data. The most appropriate basis will depend on your purpose and relationship with those involved; none is more important than the others. Which lawful basis you use for your processing will affect which individual rights are available. The ICO have a lawful basis interactive tool to help you.

The data processing must be necessary (i.e. targeted and proportionate) for your stated purpose; if your purpose can be achieved without this processing then you will not have a lawful basis.

The National Council of Voluntary Organisations (NCVO) provides guidance for charities on how to comply with GDPR.

GDPR Policies and Procedures

Accountability for data protection includes both responsibility for complying with the GDPR and being able to demonstrate this compliance. According to the UK GDPR, 'you must implement technical and organisational measures to ensure and demonstrate compliance; the measures should be risk-based and proportionate; and you need to review and update the measures as necessary'.

The ICO suggests that **larger organisations** may benefit from a privacy management framework including robust data controls, reporting structures, and assessment and evaluation procedures. For **smaller organisations**, they suggest a smaller scale approach that ensures good staff awareness of data protection, comprehensive but proportionate policies and procedures for data handling, and accurate record keeping.

All organisations should have a **data protection policy** (data protection policy template) which sets out how you deal with personal information and is applied to the collection of all new data. Someone in your organisation should be responsible for data protection too.

A **retention policy** setting out how and when you need to review, delete or anonymise different categories of information is also good practice. Small organisations that only process minimal low risk data may not need this, but still need to review and delete personal data on a regular basis (storage limitation | ICO).

A **privacy notice** helps you explain to people how you use and manage their data. People have the right to know why you need their data, what you are doing with it and who you will share it with and you are advised to write this down clearly and openly in a privacy notice. The ICO has a privacy notice template especially suitable for small organisations with suggested wording, tips and links to relevant guidance.

A **data protection impact assessment** (DPIA) helps you identify and minimise data protection risks. It is necessary for any major or high-risk data processing and is likely to be needed before processing special category data. The ICO has guidance, a template and checklist on DPIAs.

For more information on accountability measures, see accountability and governance | ICO

Resources and Support

The ICO has other helpful data protection resources for organisations including:

- A Data protection self assessment | ICO aimed at small organisations with checklists to assess your data protection compliance and suggestions for improving your personal data security
- The Data protection and coronavirus information hub which contains Data protection and employee data during coronavirus - six data protection steps for organisations | ICO

It also has a helpline for information and advice on data protection: 0303 123 1113.

Voscur is a council for voluntary service and a development agency for the voluntary, community and social enterprise sector in Bristol.

We deliver **training** on different aspects of running a VCSE organisation. Follow this link to our VCSE Academy to look for upcoming courses: **https://www.vcseacademy.org/courses/** We can also offer bespoke training for your organisation, so do get in touch to discuss your training needs.

Voscur is here to **support** VCSE organisations. For support, advice and guidance on how to apply this information in your particular circumstances, please contact us: **info@voscur.org** 0117 909 9949