DATA PROTECTION AND GDPR

Tower Hamlets CVS
www.thcvs.org.uk
info@thcvs.org.uk
Registered Charity No.1137143

This resource is aimed at VCS organisations who hold or have access to any form of personal data about either the people they work with or their employees or volunteers. This will apply to almost all organisations regardless of size. It is a vital starting point for all organisations to have a commitment to keeping personal data safe and understanding the basic principles of data protection.

What is data protection?

Data protection refers to the set of laws, regulations and processes that ensure against the misuse or publication of personal data. The main aim of data protection is to enable individuals to maintain control over how their data is held and used.

In the United Kingdom the relevant legislation is:

- The UK General Data Protection Regulation.
- The Data Protection Act 2018.
- Privacy and Electronic Communications (EC Directive) Regulations 2003.

What is personal data?

Personal data refers to any information which relates to an identifiable individual and would allow that individual to be identified either directly through that information or in conjunction with other sources of information about them.

What does the law say?

The UK GDPR 2018 sets out seven key principles of data protection:

- Lawfulness, fairness and transparency.
- Purpose limitation - information has to be collected for a specific and lawful reason.
- Data minimisation - collected data has to be relevant to the purpose.
- Accuracy - data must be accurate and kept up to date.
- Storage limitation - data should be kept for only so long as is necessary.
- Integrity and confidentiality (security) - the data should be kept safe.
- Accountability - an organisation should be able to demonstrate how it is complying with the regulations.

7 principles of data protection: A guide to the data protection principles | Information Commissioner's Office (ICO).

Voluntary and community groups have a legal responsibility to protect personal data. This legal responsibility means that organisations need to take certain steps to ensure they are compliant with the law.

Organisations need to:

- Decide upon a lawful basis for data collection.
- Identify if they are collecting special category data. This is data which is considered more sensitive than others - such as ethnic origin or medical data – and take extra precaution to ensure this data is protected.
- Ensure they do not keep data longer than is necessary.
- Enable individuals to maintain control over their own data – this includes ensuring individuals give informed consent and responding to Subject Access Requests where an individual can request a copy of all information held on them by an organisation.
- Be able to demonstrate the steps they take to ensure they comply with the law.
- Ensure that breaches of data security are reported to the ICO.

Lawful basis for data collection

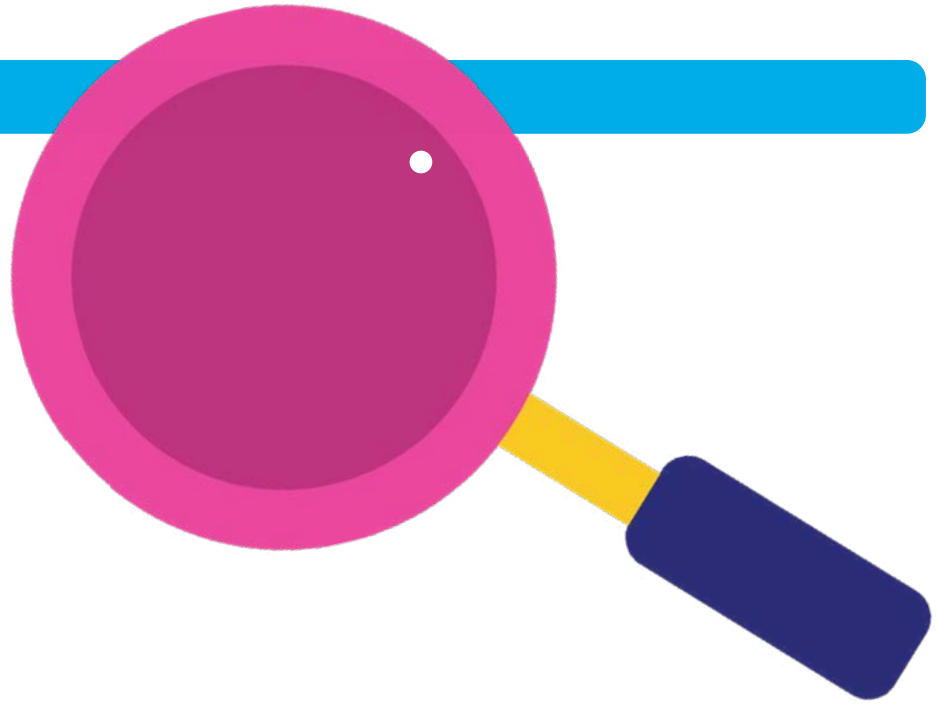
When processing personal data it is necessary for there to be a 'lawful basis' for the processing to take place. There are numerous forms of lawful basis under which an organisation can process data including:

- Consent – an individual has given you clear and informed consent to process their personal data.
- Fulfilling a contract – for example, it would be necessary to hold and process the personal data of an employee in order to fulfil their contract of employment.
- Legitimate interest – for example, information about the health of an employee or volunteer.
- Legal obligation – for example, if the organisation becomes aware of a safeguarding concern or crime that they are required to disclose to the relevant authority.

Special category data

Special category data refers to personal data that is regarded as particularly sensitive. This kind of data is subject to stricter processing laws due to the increased levels of harm that a disclosure of special category data could do to the individual involved. Forms of special category data include information about health, racial or ethnic origin, political opinion, trade union membership, and gender and sexuality.

In addition to identifying a legal basis for processing special category data organisations must also identify an additional 'condition for processing'. The ICO sets out what these are here: **Special category data | ICO.** Organisations that are processing special category data need to ensure that they take extra care and document how they are ensuring the safety of the data.



What is the ICO?

The Information Commissioners Office (ICO) is the independent regulator set up to support data protection and enforce data protection laws in the UK.
In the case of a breach of security of personal data it is the organisation's legal responsibility to report the breach to the ICO.

Data controllers and data processors
The terms 'data controller' and 'data processor' are related to the organisation or individual who is processing data and the level of responsibility they are subject to.

- **Data Controller:** A data controller is the decision maker around how and why data is collected and used. This will generally be an organisation.
- **Data Processor:** A data processor acts upon instruction from a data controller. Generally individuals within organisations are data processors.

What is a DPO?

A Data Protection Officer (DPO) is a named individual who is responsible for supporting an organisation to comply with data protection regulations. It is unlikely a small VCS organisation will be statutorily required to appoint a DPO but it may be good practice, especially for organisations who process special category data.

What does an organisation need to consider?

The first step is to carry out an information audit to find out what personal data your organisation holds and where it is. You should then know:

- What kind of data do you process? For example do you process special category data that requires a high level of security?
- Who processes that data? - Who within your organisation processes and has access to data. Are they aware of their responsibilities? Do they need training? How do you keep data safe? What systems do you use? If you keep information internally then is the information kept somewhere secure. If you use electronic systems what are their security arrangements?
- How do you process consent? Are people aware of what information you collect about them and do they give their consent for you to do this?
- Why are you collecting that data? What is the purpose for collection? If this is understood then it will be possible to identify the lawful basis for collecting data. This may require the consideration of a legitimate interests assessment.

Legitimate interests assessment

This is a process which helps organisations assess if their data processing meets the legitimate interests of their organisation whilst also balancing the rights of individuals. More information about legitimate interests assessments can be found here.

Data breaches

A personal data breach refers to a breach of security that has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Example: A list of client details is accidentally attached to an email.

An organisation needs to have processes in place that tell individuals what to do in the case of a personal data breach. This will depend on the severity of the breach and the kind of personal data that has been involved.

In the event of a data breach an organisation is required to assess the severity of the breach. The main concern is to assess the potential for any negative consequences that could happen for an individual as a result of the breach. This assessment should also take into consideration whether any special category data was involved in the breach. If a decision is made not to report the breach then this decision must be justifiable and documented.

If the organisation determines that the breach could cause potential negative consequences then there two actions they must take:

- Report the breach to the ICO within 72 hours of its occurrence.
- Inform individuals involved that their data has been compromised.

Failure to report a breach can result in a fine of up to £8.7 million or 2 per cent of the organisation's global turnover.

What does an organisation need to document?

There are certain documents that every organisation which is processing personal data will need. These documents support good practice in data protection, enable organisations to meet their legal requirements, and enable organisations to demonstrate how they are complying with the law. A checklist is provided at the bottom of this resource.

- **Privacy notice:** A privacy notice is a legal requirement. It is a publicly facing document which outlines the ways in which an organisation collects, uses, and protects personal data. It gives individuals the information they need in order to be confident that their data is secure and to be able to access and exercise control over their personal data.
- **Data protection policy:** This is an internally facing document which outlines the processes the organisation employs to ensure data is safe and that they comply with the law. It will document the lawful basis for data processing.
- **Consent:** An organisation needs to document how it obtains consent from individuals and keep a record of that consent.
- **Roles and responsibilities**: An organisation needs to document that it knows who is processing data and levels of responsibility such as if they have appointed a DPO.
- **Processing activities:** Organisations processing special category data or large volumes will need to have a record of processing activities including categories of data processed, purposes of processing, legal bases for processing, data sharing arrangements, data retention periods and security measures.

Resources

- Information Commissioners Office | ICO documentation.
- Privacy notices: Privacy notice generator - for customers or suppliers | ICO.
- NCVO - Writing a data protection policy and procedures.
- Advice for small and medium size organisations.
- Data protection self assessment - Do you need to register with the ICO? Most charities and non-profit organisations do not, but there are some circumstances (including using CCTV) that mean you need to pay a small fee and join their register.
- Children's Code - advice on data protection for organisations working with children.

Data protection documentation checklist for UK voluntary and community organisations

Document	Description	Required for	ICO guidance
Data protection policy	Explains how the organisation complies with data protection laws.	All organisations.	https://ico.org.uk/for-organisations/accountability-framework/
Privacy notices	Clear information on how personal data is collected and used.	All organisations.	https://ico.org.uk/for-organisations/advice-for-small-organisations/privacy-notices-and-cookies/
Record of Processing Activities (ROPA)	Log of what personal data is processed and why.	If 250+ staff or handling special category, high-risk, or non-occasional data.	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-of-processing-and-lawful-basis/record-of-processing-activities-ropa/
Legitimate Interests Assessment (LIA)	Assessment to justify using legitimate interests as a lawful basis.	When using legitimate interests.	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

Document	Description	Required for	ICO guidance
Consent records	Proof of valid, informed consent.	When relying on consent.	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/
Data sharing agreements	Formal agreements with third parties sharing personal data.	When sharing personal data with other organisations.	https://ico.org.uk/for-organisations/data-sharing-information-hub/
Data protection impact Assessments (DPIAs)	Risk assessments for high-risk processing.	For high-risk processing.	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
Data retention schedule	Schedule of how long data is kept and when it is deleted.	All organisations managing personal data.	https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/records-management/retention/
Security measures documentation	Summary of how personal data is protected.	All organisations	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/
Subject Access Request (SAR) Log	Record of access requests and how they were fulfilled.	When receiving SARs	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/subject-access-requests/a-guide-to-subject-access/
Data breach log	Record of breaches, how they were handled, and reported.	All organisations – required by law for certain breaches	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/breach-response-and-monitoring/assessing-and-reporting-breaches/

Document	Description	Required for	ICO guidance
Staff and volunteer training records	Evidence that people handling data understand their responsibilities.	All organisations	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/training-and-awareness/
Appointment of a data protection lead	Named person responsible for data protection (not necessarily a DPO).	All organisations	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-officers/