Newark & Sherwood CVS

COMMUNITIES 1ST

Rushcliffe Community & Voluntary Service

DATA PROTECTION

TABLE OF CONTENTS

THE DATA PROTECTION ACT 2018

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is used fairly, lawfully and transparently.

www.gov.uk/data-protection

DATA PROTECTION PRINCIPLES

Data protection principles are strict rules that anyone responsible for using personal data have to follow.

These principles ensure that the information held is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

WHAT IS PERSONAL DATA

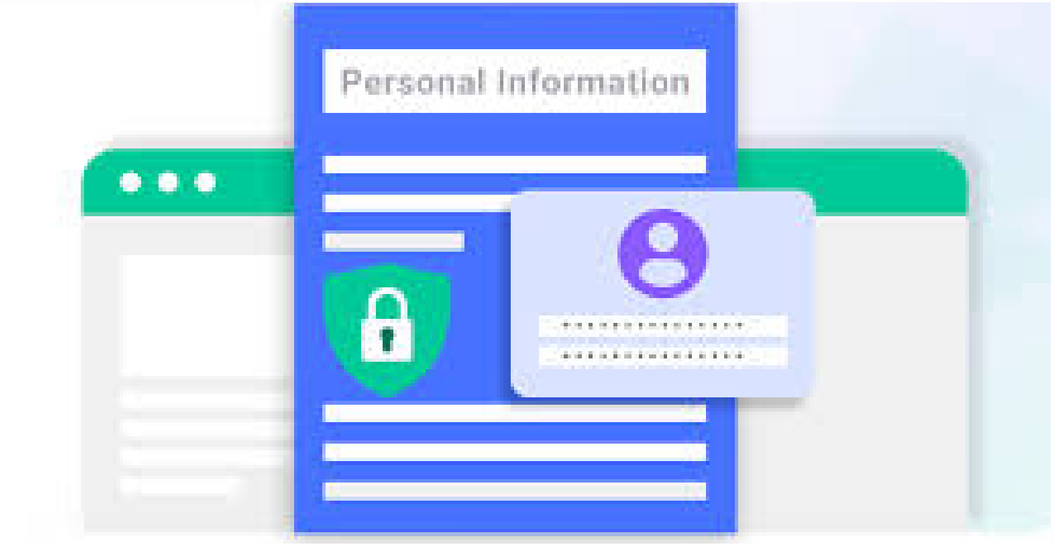
Personal data is any information held about a specific person that can make them identifiable. Examples of personal data include:

- Name and surname
- Telephone number
- Address
- Email address
- IP address (Internet Protocol)

In order to make an individual identifiable, more than one piece of personal data is needed. This could include name and IP address.

An individual can NOT be identified simply by a name, as there can be multiple individuals with the same name.

WHAT IS SENSITIVE DATA?



Sensitive data can also be referred to as special category data. This type of data is sensitive information and therefore needs a higher level of protection. Examples of sensitive data include:

- Criminal records
- Data related to racial or ethnic origin
- Medical records
- Data about religious or philosophical beliefs
- Trade-union membership
- Political stands
- Genetic data
- Biometric data
- Data related to sexual orientation
- Mental health or sexual health

YOUR RIGHTS

The Data Protection Act 2018 states that you have the right to find out what information organisations and the government store about you and how this is used.

Data subjects also have:

- The right to access personal data and supplementary information
- The right to have inaccurate personal data rectified, or completed if it is incomplete
- The right to erasure (to be forgotten) in certain circumstances
- The right to restrict processing in certain circumstances
- The right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- The right to object to processing in certain circumstances
- Rights in relation to automated decision making and profiling
- The right to withdraw consent at any time (where relevant)
- The right to complain to the Information Commission

DATA PROTECTION AND GDPR IN THE WORKPLACE

Consent

Employees must consent freely to specific use, purpose, or processing of data.
Employers must record the grounds on which they will be processing each separate category of employee data.

Organisations must demonstrate that employees were:

- Informed of the purpose and use of their personal data.
- Given a clear explanation of how it will be treated.

Accountability

Employers must demonstrate data protection compliance by training, auditing and documenting processing activities, and reviewing HR policies. They should also:

- Only collect personal data that is adequate, relevant and necessary.
- Be open with employees about data processing and allowing them to monitor it.
- Identify and limit any detrimental effects on individual privacy.

PRIVACY NOTICE

A privacy notice is a piece of written information which tells people why you need, or have their data. A privacy notice should identify who the data controller is, with contact details for its Data Protection Officer.

A privacy notice should include:

- The name of your group;
- What the data will be used for
- Which legal basis you have for using the data
- How long the data will be kept
- Whether the data will be shared with a third party, including if it will be stored on a third-party website (e.g. in Google Drive or DropBox)
- That individuals can ask to have their data removed at any time, and contact details to use to do this.

STORING PERSONAL DATA

It is your responsibility to ensure all personal data is stored securely.
It is important that you know who is storing data on behalf of your group, and that everyone understands the need to keep it secure and up-to-date. Avoid keeping data for the group on an ad-hoc basis in personal phones and address books.

Groups may store their information in different ways. Below are some examples of how information may be stored and what steps should be taken.

Computer- All computers that store personal data should have up-to-date software protection and should be password protected.

Internet- If you store personal data on the internet, you should ensure that the companies storing the data comply with GDPR regulations and that the data is not transferred outside of the EU.

Paper- If you keep personal data on paper files, you must ensure that these are locked away in a secure cabinet.

FAILING TO COMPLY WITH GDPR

Failing to comply with UK GDPR can lead to enforcement action from the Information Commissioner's Office (ICO).

The ICO can impose sanctions for these breaches which include:

- Warnings and reprimands
- Compliance orders
- Bans on processing or data transfers (permanent or temporary)
- Administrative fines

The ICO will consider a number of factors when determining the level of penalties including:

- The nature, gravity, and duration of the infringement
- The number of people affected and the extent of the damage to them
- Whether the breach was intentional or negligent
- Any previous history of noncompliance
- Any action taken to mitigate the damage
- Whether the controller notified the ICO of the infringement and co-operated

PENALTY FINES

There are two tiers of fines:

- A maximum fine of £17.5 million or 4 per cent of annual global turnover - whichever is greater - for infringement of any of the data protection principles or rights of individuals.

- A maximum fine of £8.7 million or 2 per cent of annual global turnover - whichever is higher - for infringement of other provisions, such as administrative requirements of the legislation.