



Title of policy: GDPR Extract for Volunteers
Issue number: 2
Last updated: June 2022
Policy owner: Localities Development Team

Data Protection - Extract for Volunteers

The General Data Protection Regulation (GDPR) was a law introduced by the European Union in 2018. Although the UK is no longer in the European Union, the UK has kept GDPR in UK law. It is now called UK GDPR. So, there is very little change, and the main principles, rights and obligations are the same.

The UK GDPR, along with the Data Protection Act 2018, sets out the data protection framework in the UK.

Personal data is any information that can identify a living person:

- This could be a name, initials, contact details, photograph, address etc.
- In any format, e.g., hard copy, email, electronic file, handwritten note, photos
- This may include personal data about people we support, staff, volunteers or people that work with us (e.g., supporters, donors, customers, partners, and suppliers/contractors etc.)

Some personal data is more sensitive and therefore, needs more protection. Sensitive data is data that reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sex life
- Sexual orientation
- Genetic and biometric data

Processing includes collecting, storing, reading, analysing, changing, sharing, transferring, deleting, discussing.

UK GDPR sets out seven key principles. Personal information must be:

1. Processed lawfully, fairly, and transparently
2. Only collected and processed for specified, explicit and legitimate purposes
3. Adequate, relevant, and limited to what is necessary (data minimisation)
4. Accurate and, where necessary, kept up to date (accuracy)
5. Kept in a form which permits identification for no longer than is necessary (storage limitation and retention periods)
6. Processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss, destruction, or damage (integrity and confidentiality)
7. The seventh principle relates to accountability –organisations are responsible for complying with the GDPR and must be able to demonstrate this

This means RNID must:

- Only collect personal information for a specific lawful purpose
- Only collect the information we need
- Keep it accurate and up to date
- Only keep it for as long as we need to and have agreed retention periods
- Keep it safe and secure
- Only use it for the purpose we said we would

As a volunteer you will receive personal information about people. This may be through registration, donation forms or day-to-day conversation. It is important that you keep this information safe and secure.

Personal information must not be shared with anyone outside of RNID and it must not be stored in your own personal computer, mobile devices, or filing system.

Sometimes personal information must be shared with third parties in specific circumstances (e.g., as part of our safeguarding responsibilities or where someone's life is at risk), and strict rules are in place about when this is acceptable. If you are asked to provide personal information to a third party, you must always first contact your named contact at RNID for authorisation and follow their instructions.

PERSONAL DATA BREACHES

We must report breaches to the Information Commissioner's Office (ICO) within 72 hours, and we may be reported by others. Breaches to the UK GDPR could result in action from the ICO. If you think a breach has occurred, contact your named contact RNID as soon as possible and within 24 hours.

A Personal Data breach includes:

- Any unauthorised disclosure (sharing) of the Personal Data
- Any unplanned loss, destruction/deletion, or alteration of the Personal Data
- Breaches can be accidental or deliberate

Examples:

- Sending an email containing Personal Data to the wrong person
- Leaving a document containing Personal Data on a train
- Losing an unencrypted USB stick containing Personal Data

Please think before you:

Take personal information: Do you have a reason to record the personal data?
Do you have a consent form or other lawful purpose for recording this?

Contact someone: Do you have their consent to contact them?

Share information: Do you have their consent to share information?

If unsure always contact your named contact at RNID.