

GET READY FOR GDPR IN 12 STEPS

Make sure you know all about General Data Protection Regulation (GDPR). This guide explains the basics, signposts you to further guidance, and lets you know the actions you need to take.

PARKINSON'S^{UK}
CHANGE ATTITUDES.
FIND A CURE.
JOIN US.

1. Awareness

Parkinson's UK is ensuring that everyone knows the law around data protection is changing and the impact it'll have. Staff have received online training and had a Data Protection Week to understand what the new legislation is and what it involves. They will also undergo training relevant to their job role.

We'll keep you updated as work progresses – through your staff contact, letters and email – and will signpost you to guidance and training that is relevant to your role.

2. Information you hold

Each organisation is required to do a detailed audit of its personal data. We now have an Information Asset Register, which lists all the personal info we hold and where it's stored. This is complete for the UK office.

Volunteers have been supporting us in identifying the data they collect and work with. This has given us a valuable snapshot of sensitive data they deal with and how it is stored.

We will continue to build a stronger understanding of how data flows through the charity throughout 2018. Your local staff contact will work with our data protection officer, Douglas Smith, to help build a full data picture across our volunteering network.

Think about the personal data you hold which may identify a living person. This includes name, address, phone number or email.

You may also have access to personal sensitive data through your role, for example health records, financial details, race or religious belief.

Do you process this information securely, and keep it regularly updated and accurate? Is the information only used for the purpose it was collected? If it's being used for marketing purposes, has the individual given consent for this?

3. Privacy information

The law requires us to produce a privacy notice which explains what we're doing with personal data, how we're taking care of it and how long we're holding it for. And this applies to personal data right across Parkinson's UK – from membership to JustGiving.

Our privacy notice can be found at **parkinsons.org.uk/privacy**. If someone isn't clear or you don't manage their data according to the policy, you can increase the risk of breaching data protection laws. If you'd like a printout or have a question, contact your staff contact or email **dataprotection@parkinsons.org.uk**

4. Individuals' rights

GDPR provides enhanced rights for individuals. It is crucial that if any individual enacts any of the following rights, you contact the data protection officer immediately.

These include the right to:

- be informed about the processing of your personal information, have it corrected if it's inaccurate or have incomplete personal information completed
- object to or restrict processing of your personal information or erase it
- request access to your personal information or how it's processed
- move, copy or transfer your personal information
- rights in relation to automated decision making which has a legal effect or significantly affects you

5. Subject access requests

If someone makes a subject access request, it means they'd like to know all the personal information the charity holds about them. If you receive a request like this, you must let the data protection officer know immediately. It's Douglas's role to co-ordinate the response. The law

states we need to respond to a request within one calendar month. Failure to meet these timelines results in serious consequences.

6. Lawful basis for processing personal data

The charity is required to identify the lawful basis for our GDPR activity, document it and ensure the privacy notice is updated to explain it. Here are some basics that might apply:

Data retention and deletion

You can't keep data longer than necessary. You need to inform people how long you will keep their personal data. It is crucial when we destroy data that it is done in a way that means it can no longer be used – for example, shredding paper documents or deleting digital records, not forgetting to remove them from the recently deleted folder.

Data transfer

You can only process data for the purpose it was collected. This means if you collect a name and contact details of an individual, so that they can engage in your activity, you can't use that information to allow other bodies to contact them for marketing purposes.

Privacy or data capture statements

When individuals provide you with their details, make sure you are clear and transparent about why you have them and what you will do with them. This means you need to make sure you have the right data capture statements to present to individuals when they give you their personal details.

7. Consent

We need to ask individuals to give their permission to continue hearing from Parkinson's UK – even if they've previously given their consent. We're currently going through a process of reconsenting with those people we engage with as a charity for whom we don't have sufficient consent to contact under legislation. This is something that is also happening through our local groups, and lead volunteers have already been contacted about this.

8. Children

GDPR provides additional protection for children's personal data. The charity generally doesn't process children's data. However, if you do collect children's

personal data, please get in touch with the data protection officer for further advice.

9. Data breaches

The charity is required to have the right procedures in place to detect, report and investigate a personal data breach. A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data – for example, if a person's confidential information is left lying around in a public meeting. If this fell into the wrong hands, it would be classed as a data breach – and could potentially lead to serious consequences.

Serious data breaches can result in huge fines for the charity. You need to ensure any personal data you hold is securely stored. Electronic documents should be password protected and paper files locked away in a secure place. If you discover a data breach, please notify the data protection officer immediately by emailing dataprotection@parkinsons.org.uk

10. Data protection by design

The charity is required to ensure any new data systems or processes are scrutinised against a detailed checklist to ensure there is no impact on personal data it might store. This is something that Parkinson's UK applies to all new processes to reassure those we engage with that we have taken appropriate measures to be handling their data responsibly.

11. Data protection officer

Under GDPR, we are required to designate someone to take responsibility for ensuring we adhere to relevant data protection guidelines with the ability to advise staff, volunteers and local groups. We recruited an experienced full-time data protection officer, Douglas Smith, whose remit includes supporting volunteers and ensuring they're equipped with the tools to understand and comply with GDPR.

12. International

Our Information Asset Register will take into account the possibility of any international data transfer to ensure any risk is mitigated. If you use a third party to process data please email dataprotection@parkinsons.org.uk