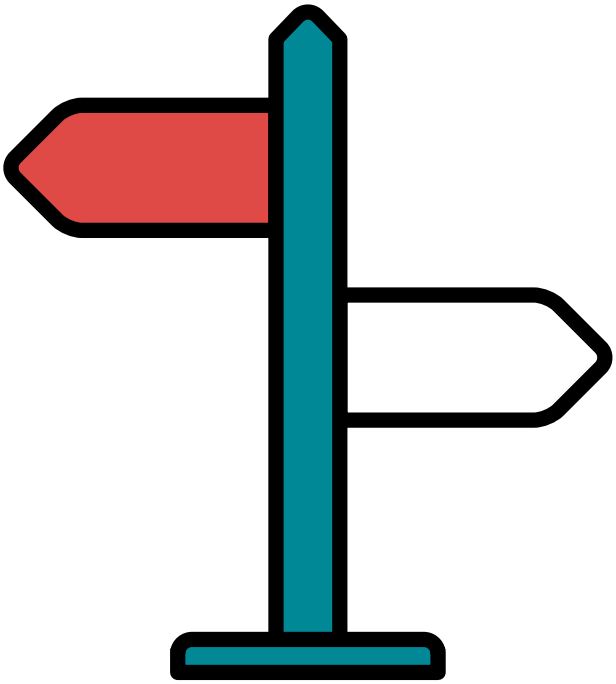
Masonic Charitable Foundation

GUIDE

The Data Protection Factsheet



This guide gives a brief overview of the General Data Protection Regulation (GDPR) to help Almoners in their wide ranging duties. It does not cover every detail of the legislation. For more detailed guidance or advice specific to your Lodge, please speak to your Lodge's Data Controller - usually the Lodge Secretary - or visit: www.ico.gov.uk.

What is data protection and why does it matter?

Every organisation or group which holds and uses information about individuals must comply with the GDPR or they risk costly fines. Ensuring personal information is accurate, up to date, kept securely and only shared with those who have permission also helps to maintain trust in the office of the Almoner and the important work linked to the role.

The legislation

The General Data Protection Regulation replaces the Data Protection Act 1998. When enforcement of the Regulation commences on 25 May 2018, it will harmonise current laws in place across all EU member states. The GDPR will continue to apply during the Brexit negotiations and it is likely that equivalent measures will be adopted post-Brexit.

Some terms explained

Data controller	The organisation that determines how and why personal data will be used.
Data processor	An organisation or individual that processes personal data on behalf of a data controller.
Data subject	An individual who is the subject of personal data.
Personal data	Any information relating to an identified or identifiable natural person. It includes, for example, name, date of birth, and opinions about the individual.
Sensitive personal data	Defined by the Regulation as information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union Membership, genetic data, biometric data, data concerning health, sex life or sexual orientation.
Processing	Any use to which personal data are put, including: • Obtaining and retrieving • Holding and storing • Making available to others within or outside the organisation (including sending by email) • Printing, storing, matching, comparing, destroying
The Information Commissioner's Office (ICO)	The UK's independent public authority set up to uphold information rights. It is responsible for data protection in England, Scotland, Wales and Northern Ireland and enforces and oversees legislation including the GDPR.

Key principles of Data Protection

- Data is processed lawfully, fairly and in a transparent manner.
- Data is obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data processed is adequate, relevant and limited to what is necessary.
- Data is accurate and, where necessary kept up to date.
- Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Data processed in accordance with the data subjects' rights.
- Data processed in a way that ensures appropriate security of the personal data.

- Data not to be transferred to a third country or to an international organization if the provisions of the Regulations are not complied with

What does this mean in practice: some simple steps to take

- Let people know what you intend to do with their data: they should know why you need their data, what you are going to do with it, how long you will keep it and who it is going to be shared with. This information can be given verbally or in writing.
- Only collect the data you need to do what you are doing. Don't collect extra information 'just in case'.
- Let people know they have the right to correct any data if it's wrong and how to let you know if they decide they don't want you to use the data anymore.
- Share the data you hold about an individual with them if they request details.
- Only keep data for as long as it is needed. Have a schedule for reviewing and deleting information and follow it.
- Ensure the data you have is kept up to date. If possible, take a moment to check and update records with individuals whenever they contact you.
- The data you collect can only be used for the purpose(s) you gave when you collected it. For example, you wouldn't be able to send a fundraising request to someone who has provided their details so they can be sent details of upcoming fellowship meetings.
- Make sure you have a strong password on files and portable devices. Use symbols and lower and upper case letters.
- If you plan to store information on laptops, and other devices consider installing a remote 'wiping' solution that will delete your hard drive in the event it is stolen.
- Shred paper files before throwing them away and make sure that files have been permanently wiped from laptops, computers and other devices before you get rid of them.
- Make sure you are the only one with access to the email account you use for your Almoner duties. Do not use a joint account with a wife or partner.
- Be careful when sending information outside of the UK. It is unlikely that an Almoner will need to do this so always get the agreement of the person concerned before you do. Remember other countries do not have the same level of protection for personal data that we do.

Useful contacts

- **The Information Commissioners Office:** https://ico.org.uk/
- **GDPR Portal site:** http://www.eugdpr.org/eugdpr.org.html