Data protection

The General Data Protection Regulation (GDPR) and The Data Protection Act (2018) came into force in May 2018. Together they represent the biggest change to data protection legislation in a generation. Please follow the information in this section to ensure you understand what this means for your WI or federation.

Why is this legislation needed?

The UK GDPR was created to reinforce the protection of personal information as a fundamental right. The main aims of the regulation are to:

- Empower individuals to take more control of their personal data by giving them stronger rights; and
- hold the organisations who collect and store personal data accountable.

The UK GDPR should be read in tandem with the Data Protection Act 2018 (DPA) which replaced the 1998 Act.

Fundamental rights under the UK GDPR

People have the following rights:

- Right to be informed about data processing
- Right to access their personal data
- Right to rectify any incorrect personal data
- Right to erase personal data
- Right to restrict processing
- Right to data portability
- Right to object to data processing
- Right not to be subject to automated decision-making

DPA Principles

Personal data shall be:

1. Used fairly and lawfully
2. Used for limited, specifically stated purposes
3. Used in a way that is adequate, relevant and not excessive
4. Accurate
5. Kept for no longer than is absolutely necessary
6. Handled in accordance with people's data protection rights
7. Kept safe and secure
8. Not transferred outside the United Kingdom

What is personal information?

Personal information is information that identifies an individual such as:

- **Name**
- **Address**
- **Phone numbers**
- **Bank details**
- **Photos and videos**

Personal information that is especially sensitive is called **special category information**. This requires explicit consent from the individual to allow processing. For example information about an individual's:

- **Race and ethnic origin**
- **Political and religious beliefs**
- **Health, both mental and physical**
- **Trade union membership**
- **Sex life and sexual orientation**

Personal information can be stored electronically (e.g. the MCS) or physically (e.g. in a locked drawer).

What does your WI need to do to comply with this legislation?

WIs process personal information about individuals to provide membership services and to operate efficiently. We therefore need to ensure this processing is carried out in accordance with data protection legislation. Every new member of your WI must fill out the WI Member Registration Form produced by the NFWI to ensure their data can be lawfully used by all levels of the organisation to administer their WI membership. If your WI collects and processes personal information not covered by the standard form, you might need to provide your members with additional information on how their personal details are used.

A common example would be if your WI is planning on taking photos and/or videos of your members it is best practice to ensure they have signed a photo and video consent form, if they are happy to do so (members are not obliged to give consent for photos and/or videos).

A suggested photo and video consent form, produced by the NFWI as well as the latest WI Member Registration form can be found at the bottom of this page, as well as other documents which will allow your WI to act consistently with the UK GDPR.

In accordance with the principles of accountability and transparency, WIs also need to be able to demonstrate that they understand how they process personal data and why they do so. They also need to document any consent given by members for such processing to take place.

Your WI needs to know and document the following (known as data mapping):

1. What personal information do you have about members?
2. How did you get this personal information?
3. Who has access to this personal information?
4. Why do you need this personal information? (legal basis for processing)
5. How long are you going to keep this personal information for?
6. Who will the personal information be shared with? Who has access to this personal information?
7. How will you dispose of the personal information when you no longer need it?

The above information needs to be communicated to the individual whose data you are processing (known as a privacy policy).

Other changes

Subject Access Requests – If a member requests to see the personal information your WI holds about them this is known as a Subject Access Request. This information must be provided to the individual without delay and in an accessible format.

Assessing Risk – When your WI carries out a new project you need to assess the risks involved with any personal information that will be used for the project.

Information Breach – If personal information is:

- accessed by an unauthorised person;
- altered;
- destroyed;
- lost; or
- disclosed incorrectly

then an information breach has occurred. Your WI must have in place adequate procedures to detect, report, investigate and manage an information breach.

Support from the NFWI

We are here to support your WI in your work to ensure compliance with the UK GDPR and DPA. We strongly encourage your WI to go through the below resources to get an overview of the new legislation and find out what you need to do. As always our staff are on hand to help with any queries and concerns.

If you have any questions please email dataprotection@nfwi.org.uk

The Information Commissioner's Office

The ICO is an independent supervisory authority that regulates privacy laws in the UK and has the ability to enforce sanctions and fines on organisations that do not comply with the GDPR. They are continuously developing helpful guidance on data protection. Some helpful resources include:

Guide to Data Protection

Electronic Marketing