May 2018

Getting ready for the General Data Protection Act (GDPR) – WIs and federations

This document will help prepare your federation or WI for the General Data Protection Regulation (GDPR) coming into force on 25 May 2018.

The WI Member Registration Form, letter to all WI members and NFWI Privacy Policy explain that the WI will use the personal details a member provides to administer their membership (and if the member is an officer, a committee member or has another role that position). However you will still need to be aware of the personal data you process, why, how long you retain it for etc. and ensure that you have the relevant technical and organisational measurers in place to protect it.

For personal data you process that falls out of that scope you will also need to consider and document your lawful basis and, if necessary, proof of consent etc. You will also need to ensure that you are transparent with your data subjects (or individuals whose personal data you are processing) and make any additional processing activity known to your members.

For your reference useful data protection definitions have been included at the end of this document.

1. Introduction

The General Data Protection Regulation (GDPR) is the biggest change to privacy law since the Data Protection Act (1998). At the core of GDPR is transparency – ensuring your data subjects know what information you collect, and what happens to it. It's only possible to be fully transparent if your federation or WI fully understands the data it holds and what it does with it.

This guide starts off by providing a number of practical steps to consider before going into some of the key points of the regulation in more detail, with WI-specific examples where possible.

2. Practical steps

Please consult the **GDPR - Practical steps and examples for federations and WIs** guide for WI-specific interpretation and application of the GDPR.

3. Lawful GDPR bases

To ensure your processing of personal data is lawful, you need to identify the most appropriate lawful basis for your personal data and special category data. Please note that it is important that you consider these carefully as it may be difficult to change from one to another at a later date. If you need any help doing this, please get in touch.

For the personal data you are processing, you have the following lawful bases to choose from:

- **CONSENT**– the individual has given their consent to the processing of their personal data
- **CONTRACTUAL** – processing of personal data is **necessary** for the performance of a contract to which the individual is a party or to take pre-contractual steps at the

request of the individual

- **LEGAL OBLIGATION** – processing of personal data is **necessary** for the compliance with a legal obligation

- **VITAL INTERESTS** – processing of personal data is **necessary** to protect the vital interest of the individual or of another individual (save someone's life)

- **PUBLIC TASK** – processing of personal data is **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority

- **LEGITIMATE INTERESTS** – processing is **necessary** under the legitimate interests of your WI or federation, or a third party, unless these interests are overridden by the individual's interests or fundamental rights

In order to determine the most appropriate lawful basis, you need to think about the purpose for processing the personal data and the relationship you have with the individual. There is no basis that is better or more important than others.

To help you get started ask the following questions:

1. **Is the processing necessary?** The processing is necessary if it is targeted and a proportionate way of achieving your purpose.

2. **Do you have a clear purpose for processing the personal data?** If your purpose is clear-cut and it relates to fulfilling a legal obligation, performance of contract, or protecting someone's life (vital interests) or public task, then these lawful bases should be considered first.

If you process data for other purposes you may want to consider using either 'consent' or 'legitimate interests' as your lawful basis. Choosing 'legitimate interests' would keep you in control of the processing but you need to be able to demonstrate that individuals expect this processing to take place, and that it will not cause them 'unwarranted' harm. You will do this by completing a Legitimate Interests Assessment (LIA). Choosing 'consent' may be the more appropriate lawful basis if you would like to give individuals responsibility and control over the data, and allow them to with draw their consent at any time. Please note that the GDPR sets higher standard for consent. You need to keep a record of **who, when** and **how** the individual consented, and **what** the individual was told at the time. The information you give to then when collecting their data needs to be clear and specific and reflect the different processing activities and stating any third parties that will rely on the consent. The consent needs to be separated from other conditions, and you must tell individuals how they can withdraw their consent. Your consent will require a positive action by the individual to opt in.

If your existing consents are not in line with the GDPR, you need to **refresh** them before 25 May 2018.

You can read further about consent and the other lawful bases here.

In addition, the ICO has produced a helpful lawful basis interactive guidance tool to help you decide your lawful bases and/or confirm your decisions.

Please note that if you send individuals (e.g. members) marketing emails that for example include information about WI activities and campaigns, you need to ask individuals for their consent so that you are compliant with Privacy and Electronic Communications Regulations 2003 (PECR). Further information can be found here.

Individuals will also have different rights under different lawful bases. Identify which rights would apply, and make sure that your WI/federation or you can accommodate fulfilling these rights when choosing the most appropriate lawful basis:

- Right to be **informed** (transparency) – privacy notices
- Right of **access** – subject access requests
- Right to **rectification** – if data is inaccurate or incomplete
- Right to **erasure** – 'right to be forgotten' under certain circumstances
- Right to **restrict processing** – storage only
- Right to **data portability** – moving data from one IT environment to another
- Right to **object** – includes right to object to direct marketing
- Rights in relation to **automated decision making** and **profiling**

The table below gives you an overview of individuals' rights in relation to lawful basis. Please note that this is not an exhaustive table.

	Right to erasure	**Right to data portability**	**Right to object**
Consent	Yes	Yes	No, but right to withdraw consent
Contract	Yes	Yes	No
Legal obligation	No	No	No
Vital interests	Yes	No	No
Public task	No	No	Yes
Legitimate interests	Yes	No	Yes

Further information about the rights of individuals can be found here, and you can always contact the NFWI for assistance.

If you process special categories of personal data you are required to identify two lawful bases for this processing. This is because special category data is more sensitive (higher risk) has stronger legal protection. You should choose your first lawful basis from the ones mentioned above for personal data (general processing). Your second lawful basis should be chosen from the alternatives listed here.

Please note that the Data Protection Bill is proposing additional conditions and safeguards for special category data. This legislation is currently being discussed in Parliament and further guidance will be issued shortly. In the meantime, please contact the Data Protection Team for further information.

1. Transfers of personal data (outside of the EEA)

The GDPR applies within Europe, and should apply to European citizens when their data is processed overseas, however data protection laws do differ outside of Europe so if you do have information stored abroad it is important to be transparent and let people know.

For federations and WIs you will need to think about your email accounts, websites and any cloud-computing services you use (Office 365 for example).

2. Retention times and retention procedures for your personal data

The GDPR requires you to state specific retention times/retention criteria for your personal data in your privacy notices, and develop retention procedures to enable your WI/federation or you to comply with these.

3. Update (or create) a privacy notice

Your privacy notices allow you to communicate directly to individuals when you are collecting their data why you are doing so and how you intend to use it. In order to comply with the GDPR, they need to be updated to include the following:

What information must be supplied?	Data obtained directly from the individual	Data **not** obtained directly from the individual
Who you are and your contact details	✓	✓
Why you are processing the data and its lawful basis	✓	✓
Your legitimate interests where applicable	✓	✓
Categories of personal data	✓	✓
Any recipient or categories of recipient of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with the Information Commissioner's Office (ICO)	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

Your privacy notice should be concise and easy to read and to access. You can use the latest NFWI Privacy Policy as a starting point: https://www.thewi.org.uk/privacy-policy

4. Useful data protection definitions

GDPR (General Data Protection Regulation)	General Data Protection Regulation (GDPR) is an EU law that will replace the Data Protection Act (1998) from **25 May 2018**.
The GDPR Principles	Personal data shall be: • Processed **lawfully, fairly** and in a **transparent** manner • Collected for **specified, explicit, and legitimate purposes** • **Adequate, relevant and limited** to what is necessary • **Accurate**, and where necessary, **kept up to date** • Retained **only** for as long as necessary • Processed in an appropriate manner to maintain **security** ***New accountability requirement:*** *You need show **how** you comply with these priniciples*
Personal data	Personal data is any information that can be used to identify an individual, such as names, addresses, telephone numbers, email addresses and financial details. Personal data can be an individual that can be identified in a photograph or in a video recording. It can be electronically stored on a computer or on other electronic devices including a USB stick or manually stored on a piece of paper in a cupboard. **Please note** that personal data also applies to personal information about individuals in their professional capacities. The fact that they are acting in an official capacity means that they are more likely to expect you are processing their personal data.
Processing	Processing is a broad term and includes anything that you do with personal data, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise make available, aligning or combining, restricting, erasing or destroying.
Special category data	Special category data has greater legal protection and is personal data revealing race or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation.
Data controller	A data controller is a natural or legal person or organisation which determines the purposes and means of processing personal data. **Example:** The NFWI is a data controller because it determines what personal data is collected when new members join the WI (and complete the WI Member Registration Form) and the purpose for which this information is used (to administrate the WI Membership).
Data processor	A data processor is a natural or legal person or organisation which processes personal data on behalf of a controller. **Example:** Mail International is the mailing company that sends out the WI mailing to all WI Secretaries. For this purpose, the NFWI (data controller) send Mail International (data processor) the names and the postal

	addresses of all WI Secretaries. Mail International is therefore processing personal data on behalf of the NFWI.

5. Further reading

If you would like to find out more the best place to start is the Information Commissioner's Office Website, specifically https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/