May 2018

Getting ready for the General Data Protection (GDPR) - Practical next steps and examples for federations and WIs

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.

What do I need to do?	How do I do it?
a. Understand the personal information you hold	
You need to identify the personal information that your federation or WI holds. You also need to document where it came from, how you obtained it, how it is used, who can access it, where it is stored and how long it is retained for.	Create a "Data Map". The NFWI has provided an Excel Data Mapping template to assist you with this.
Consider the lawful bases for processing personal data, and the Data Protection Principles to the data you hold.	Follow the guidance in the "Decide on the appropriate lawful bases" and "Data Protection Principles" sections of the full WI/federation GDPR guide. The NFWI has also provided a Legitimate Interest Assessment (LIA) template to help determining the validity of Legitimate Interest as a lawful processing basis.
Access the risk to harm to the data subject, and if necessary undertake Data Protection Impact Assessments.	Refer to the Information Commissioner's Office (ICO) guidance - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
b. Document your processing activities	
Create relevant documentation demonstrating your understanding and compliance of the regulation.	Ensure that the steps you have taken to comply with GDPR are documented. You will also need to demonstrate that you are

	consistently applying best practice, this means continually considering the privacy of data subjects. GDPR isn't something that can be prepared for and forgotten, it is a continuous journey.
Demonstrate accountability.	Document the basis for the choices you have made.
c. Apply appropriate technical and organisational measures	
GDPR applies to paper as much as it does to information held online. It's important to ensure all personal data is retained safely and securely, and that you have mechanisms in place to ensure it is processed and held in the ways you outline.	Data should be kept securely. In a practical sense that means you should ensure paperwork is kept securely locked if it needs to be retained, and that you should take appropriate security measures for example ensuring that the computer you use to process personal information is kept updated, has security software installed and is password protected. Organisational measures include knowing how to deal with a data breach, or a Subject Access Request (SAR) for example.
You should ensure a level of security appropriate to the level of risk.	Data should be secured in a way appropriate both to your circumstances and the risk your processing poses. The regulation acknowledges that there is no "one size fits all" solution. For example a health centre holding a record of an individual's medical history, or a bank holding detailed financial information both pose very different levels of risk to the information commonly held by a WI Secretary. You should be confident that the measures you take are appropriate for your charity.
d. Consider third party relationships	
Does your WI share any data with third parties?	Third parties might include other local groups, cloud computing service providers or printing companies, amongst others. If you process personal data via a cloud service it might be hosted outside of the European Economic Area. Any company delivering a service to EEA citizens should be GDPR compliant, but you need to be diligent and check – and let people know if their data is leaving the EEA.

	Closer to home you might be sharing personal data with other local groups, or even with printing companies. If you are you'll need to be clear what they are doing with the data you share as well.

Examples:

1) **My federation uses a cloud-based email service (such as Office 365) to ensure that all staff, officers and WIs have a branded email address that the federation can control. In order to do this we must share personal information (names) with the cloud provider. That information may then be transferred to the United States, and emails themselves are likely to contain additional personal information.**

   The first step is to document the above in your federation's Data Map, this is the first step towards demonstrating that you **understand the personal information you hold**.

   Secondly you would want to ensure you understood the lawful basis you were relying on for this processing activity. If your federation has decided that ALL staff, officers and WIs must use your email system then **consent** is unlikely to be appropriate (consent must be freely given, so if there's no choice there can't be consent). With consent ruled out you might next want to consider your federation having a **legitimate interest** in having a consistent email service across your federation. A Legitimate Interest Assessment (LIA) will help confirm this.

   Using cloud-based email from a reputable supplier such as Microsoft makes sense, it's cost-effective, secure and a lot less hassle than having numerous email suppliers, however you need to be sure that you **document your Processing Activities** to demonstrate how you comply with GDPR etc. With our example of cloud-based email you will find that all large providers are sharing plenty of information demonstrating the steps they have taken to make their services GDPR-ready.

   Switching to cloud-based email can be a good example of **applying appropriate technical and organisational measures**. Having a reliable service controlled and maintained by a federation is a lot safer than having individuals create and maintain their own email addresses. It puts the federation in charge of the data.

   A cloud-based email provider would be a third party processor, so your federation would need to consider the **third party relationship**. As mentioned above all the major providers will have policies available relating to GDPR to reassure you that your data is safe with them, however it's important to review these documents – make sure you understand processes for removing old accounts, how you could use the service to help comply with a Subject Access Request, and of course consider where the data is stored. A lot of cloud-based services replicate data across the world, so copies might be stored in Amsterdam and might be stored in Seattle and New York as well. If there's the possibility that data will be stored outside of Europe then it's important this is communicated to those using your service.

2) **My WI shares member details with different members, as different people are responsible for organising different trips and events. Can we still do this?**

In this instance you would again start by completing the data map to help **understand the personal information you hold** and who has access etc.

To help determine **the lawful basis for processing** the information you would again want to look at the various lawful bases. In this example we can probably once again rule out all but having a **legitimate interest** in processing information in this way, and **consent**.

Once again, you might decide that consent isn't the best fit – firstly because again members don't really have a choice, having information shared with different people is simply the way your WI is structured, and secondly because of the complexities of different people having to monitor consent it's likely to be very difficult to ensure the consent remains valid.

It's also important to remember that existing legislation, the Privacy and Electronic Communications Regulation (PECR), which sits alongside the GDPR gives individuals specific privacy rights in relation to electronic communications states that you must have consent to send marketing emails.

When considering **appropriate technical and organisational measures** you will want to think about the procedures you have for sharing personal information across your WI and potentially with third parties. If multiple people store personal data are they all keeping it securely?

When **considering third party relationships** you will need to consider how you keep members informed. Do you use an online tool such as MailChimp? Do you share member details with hotels, travel agencies, coach companies etc.?