

# GDPR

## General Data Protection Regulation

May 25<sup>th</sup> 2018

We do need to give you information about a new law that will affect us all. On May 25<sup>th</sup>, the EU will launch the GDPR, the General Data Protection Regulation. **It concerns personal data, data that can be attributed to an identified person. We handle such data and, therefore, must comply with this law.**

We have an obligation to tell you about the GDPR because Group Leaders necessarily have access to some of the data. **You too have to comply with the new law.** You need to know what we are doing to ensure that we are compliant and you need to know what you have to do. And anyway, as members, you are entitled to know what data we collect, why and what we do with it.

Fear not though, once past the bureaucratic legal verbiage, the practical implications for us are straight forward. Happily, our needs are simple. Google or Facebook we are not! We have to change some practices and processes but, collectively, we all just need to be sensible.

**I will talk about it but this is not a legal lecture. I am not a lawyer. I will be giving you only an overview. Ask questions whenever you wish, now or after the meeting.**

### **Why do we need your personal data?**

- **In order to provide EU3A activities and services to you.**
- **For the administration, planning and management of EU3A.**
- **To communicate with you about group and other EU3A and national U3A activities.**
- **To monitor, develop and improve the provision of our U3A activities.**

The law is all about the member data that we collect. What we collect, how we do it and what we do with it when we have got it. We need just enough data about each member to be able to run the organisation. We need name and address, telephone number and/or email address. That's about it!

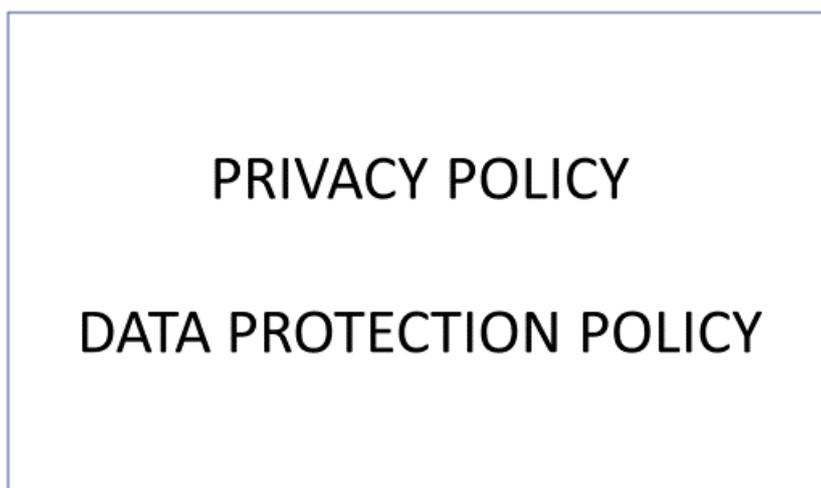
### **A CONDITION OF MEMBERSHIP**

- **Name, address, tel nos,  
email address**
- **But not "sensitive"  
information**

Without that data we simply cannot function. If someone does not want to supply it to us or, having done so, won't allow us to use it, we now say that **they cannot be a member!**

**So, there is a change:** in order to be able to comply with GDPR we are now saying **“No data, no permission to use the data, you cannot join as or continue to be a member”**. **New joiners will be asked to agree to this when they apply and existing members will be asked at Renewal time.**

We don't want “sensitive” personal data. There may be times when we need some at the most innocuous end of the scale. Say DOB for example, for a travel company for a trip abroad. If so, “we” will ask the affected members for explicit permission and won't keep the data once it has served its purpose. “We”, in such cases is likely to be one of you. If it is, say **in writing** what data you want, why and what will happen to it. And once it has served its purpose, destroy it!



To formalise what we have to do, we have introduced two policies, Privacy and Data Protection. Copies of them have been placed on the web site, in the Welcome section. I don't propose to wade through them now, they are there for you to read at your leisure. Please do and feel free to ask about them and comment on them at any time.

### **PROTECTING PRIVACY BUT WE DO NEED TO SHARE DATA**

**Internally** - with Committee members, authorised technical support and group leaders

**Externally** – an external management system (Beacon), direct mailing for *Third Age Matters* and EU3A's newsletters. We judge their digital and physical systems and procedures to be secure.

**If we have a duty** to disclose it for HMRC and other legal and regulatory reasons.

**Group Leaders** are necessarily less private

**How do we comply with the need to protect privacy?** We limit the people in EU3A who have access to the data. Access is role dependent. For example, Group Leaders need access to a limited subset but do not need and will not have, access to all of it. The data is kept in a database which is part of the Beacon system and Beacon allows us to specify in some detail who is allowed to see what. We can specify “roles” and attach to each of them a detailed set of “privileges”, that is we can tell Beacon what someone in this role is allowed to see and what they must not see. Group Leader is one such role.

Some third parties need access to some of it – in visitor lists for some outings, in distribution lists for the distributors of TAM and our Newsletters, our auditors, HMRC and other authorities if necessary. We do have an obligation to check that what they do and how they do it allows us to remain compliant.

Group Leaders are necessarily less private than other members. We do need to share their contact information more widely. Members need to be able to contact them. We do not publish their contact details on the web since that is open to the public. We do publish them in Beacon, accessible only by members. We do publish them in our Newsletters and the Bulletins, distributed only to members (*but we can't guarantee no leakage*).

## **DATA PROTECTION**

**Implementing the policy ensures that we:**

- **Comply with data protection law and follow good practice.**
- **Protect the rights of members, suppliers and partners.**
- **Are open about how we store and process member data.**
- **Protect ourselves from the risks of a data breach.**

**How do we comply with the need to protect the data?** The Data Protection Policy requires us to take good care of the data. We do. For example, we keep our database on a secure third party server accessed by secure communications links. Where we need to share data between Committee members outside Beacon, we use a secure file sharing system.

**HOW LONG DO WE KEEP THE DATA?**

**IT NEEDS TO BE CORRECT AND UP TO DATE?**

**MEMBERS NEED TO BE ABLE TO CHANGE IT?**

We don't want to hold on to data any longer than we have to but HMRC requires us to keep some data for 6 years.

There is some data that we are not allowed to keep. The Membership Secretary has made a sweep through the current database and through the Pre Beacon spreadsheets, deleting emergency contact (aka NOK) data for everyone who has left us. Why? Because we have no "legitimate interest" in it.

We endeavour to keep member data up to date and accurate, asking members at least three times a year to check it and we give them the means to check and edit it on-line at any time.

## GROUP LEADERS

### KEEP MEMBER DATA SECURE

- If using Beacon **DO NOT USE PUBLIC COMPUTERS**
- If not using Beacon
  - Use BCC for emails
  - Obtain explicit consent from members before showing their data to other members
  - Obtain explicit consent from members if their data is to be shown outside the group (e.g. for visits). Destroy the data afterwards.
- Update the Membership Secretary's Records

**To comply, what do you need to do?** Better for you to use Beacon but if you choose to stick to pieces of paper, take care who sees them. Use BCC's when you send emails unless your group's members explicitly agree that they can all see each other's information. Help us keep the data up to date, letting us know if member's details change.