London Region of U3as

# SHARED PRACTICE GUIDE 014 – GDPR COMPLIANCE

**Rev 02**

## 1. Introduction

Shared practice guides (SPG) are vehicles to share knowledge between the u3as in the London area. They are created by collating knowledge and experiences from those u3as. They are only a guide – what worked for one u3a might not work for your u3a. If in your experience something is wrong or you disagree with something in this SPG, please write in to allow an update to be created and published. It is hoped these Guides will grow over time with more shared experiences.

## 2. Scope

This particular SPG addresses the aspect of General Data Protection Regulation (GDPR) and the compliance with this regulation. Members' personal data should always have been a concern for u3as but the new regulation certainly puts a focus on this topic. This SPG assumes that a u3a has already set up its documentation for initial GDPR compliance. The SPG is to be used for periodic audit of that documentation and the application of its stated intent.

Overall the risk needs to be remembered – the risk of personal data being hacked or inadvertently shared with non authorised bodies. To lower this risk, the extent (quantity) and spread (over various locations) of such data, should be minimised.

## 3. Background

The GDPR legislation was tabled in 2017 and come into effect in 2018. There was great activity at the time to understand what this new regulation meant and what organisations had to do to become compliant. However, following that initial awareness and burst of activity for most organisations, including u3as, the level of attention has subsided – understandably. But there should still be some level of ongoing awareness and concern regarding the topic. Appendix 1 provides a checklist that can be used to audit a u3as compliance with its own data protection documentation and hence GDPR.

## 4. Learnings

In time it is expected that, through use, there will develop further learnings leading to updates of this SPG.

General considerations arising to date: it is a good idea if the audit can be done by an 'independent' person, ie someone different to who ever possibly set up your Privacy Policy etc in the beginning. So that it's a 'cold eyes' review. Possibly a new Committee member, a new Trustee would serve this purpose.

Another point arising – use of 'cookies'. Thoughts on this developed after the first flush of compliance with GDPR. Consider use of cookies for all Systems you use but particularly your website programme. Develop a separate Cookies Policy.

## 5. Documentation

It is assumed that an individual u3a will have base specific data protection documents in place. These should include:

i. Data Protection Policy
ii. Privacy Policy/ Statement
iii. Cookies Policy (if not coved within Privacy Policy)
iv. Legitimate Interest Agreement (if required)

v. GDPR Declaration (optional)

Templates for the first three can be found on the Trust's website (see References below). There is a template for the 4th element in Appendix 2. The above is the minimum documentation necessary. Appendix 3 lists some other documents that should be considered for creation.

## 6. Systems

### 6.1. Membership Systems

Consideration needs to be given to where personal data is being recorded. Some u3as might be using Beacon which is principally for storage of members' personal records but other u3as might be using other membership systems, MS Excel spreadsheets or even manual registers. Beacon is GDPR compliant.

The audit should check that this membership data is being recorded ideally only once, in one system (avoiding duplication). Also consideration needs to be given to the access to this data. For example Membership Secretaries will obviously need full access, including amending membership data when required; other post-holders might need to use some of the data, but not amend it. It is probably wise also to have a back-up person for each data-user. It needs to be clear who else needs / has access to that Membership data. Clarity is also needed about who controls the access permissions to such data sources and whether this can this be minimised.

Particular care needs to be taken regarding succession and handover especially between committee members but also at Group Leader/Coordinator level. Part of the handover process from one person to another should be the clear requirement that the resigning member confirms they have/ are deleting all records of members' personal data. This should include emails – which will carry as a minimum members' email addresses.

### 6.2. Event Systems

Your u3a may organise events for your members and use a company providing a proprietary event booking system (eg Eventbrite, Wufoo or similar). These systems will take and store members' personal data. Before utilising such a company you need to ensure they are GDPR compliant. If so they will have their own policies for minimising storage of personal data. There is no facility for the user to delete previous records held within the system. However you should ensure your Event Organiser(s) delete any downloaded information for a particular event (ie registration records).

### 6.3. Mail Systems

Your u3a may utilise a mass mailing system, particularly if it doesn't use Beacon. For example Mailchimp. As mentioned above for organised events, companies providing mass mail systems such as Mailchimp will be GDPR compliant. However, you need to check to ensure they are GDPR compliant. They will then have their own policies for minimising storage of personal data and will probably have an 'unsubscribe' facility. But this does not delete previous records held within the system. Your administrator will be able within these systems to delete their records. In fact there will be quite an effort necessary to constantly ensure that the records and contact details, for past members are removed. Checks on the frequency and methods used to do this should be part of an audit.

### 6.4. Public Facing – Websites, YouTube

It is good practice to ensure no member personal data is visible outside your u3a. So any websites, leaflets or documents to be used in the public domain should not show personal email addresses or phone numbers or home addresses. 'Legitimate interest' is not a basis for needing to expose personal details to the public. Setting up 'alias' email accounts for key positions is a useful practice so that those alias mail addresses can be exposed to the public domain. (They are also useful for succession.)

Similarly if any recordings are taken and posted on YouTube or other internet systems, no personal data should be visible.

Note: Sitebuilder for websites have a published Privacy Policy (which includes the use of cookies).

### 6.5. Cloud Storage System

Your u3a may use a cloud storage system for filing for example minutes of meetings and amongst other records. These will contain personal data, eg names and possibly email addresses. These proprietary systems will be GDPR compliant but you should check for your chosen system that they are GDPR compliant. They will then have their own policies for security of data. However you will be the party to define what you put into a cloud storage system so you will need to consider the risk and minimise the extent of personal data held in such a system (eg it shouldn't hold copies of attendance records or information also held in another system).

### 6.6. Zoom

Your u3a may use Zoom (or other conferencing systems) for online meetings. You should check that this proprietary system is GDPR compliant. They will then have their own policies for security of data. They should then have their own policies for minimising storage of personal data. But they do not delete previous records held within their system. You can produce reports from Zoom on attendance at any or all of your meetings. This may show names or personal email addresses – depending on what the participant enters when setting up their Zoom account or what they use to 'Name' themselves on screen. If any of these available reports are downloaded (ie exported) then the management (ie access, handling and storage) of them needs to be considered. The reports should generally not be retained long term. Checks on the frequency and methods used to do this should be part of an audit.

## 7. Data Accessibility

To reduce the overall risk of data leakage, as well as minimising the extent of data held, consideration also needs to be given to minimising who and how many people have access to this data. At the lowest level, for example, emails should not expose personal email addresses. All emails should be 'blind copied' to members or be issued by a 'System' like Beacon or Mailchimp which automatically hides addressee email addresses from others.
Sometimes within Interest Groups, the group members may want to communicate with each other. This could be by email, or personal mobile phone numbers for Groups that use WhatsApp or similar. If Group Leaders / Coordinators have individual recorded consent from all members of the group, then this can be classed as complying with legitimate interest requirements.

Even at committee level consideration needs to be given to who has access to which systems. Not all committee members will need to access all systems.

Records should be kept about who holds passwords to the various systems. Back-up is required but passwords should not be available to many. Details of any password management system used should also be kept.

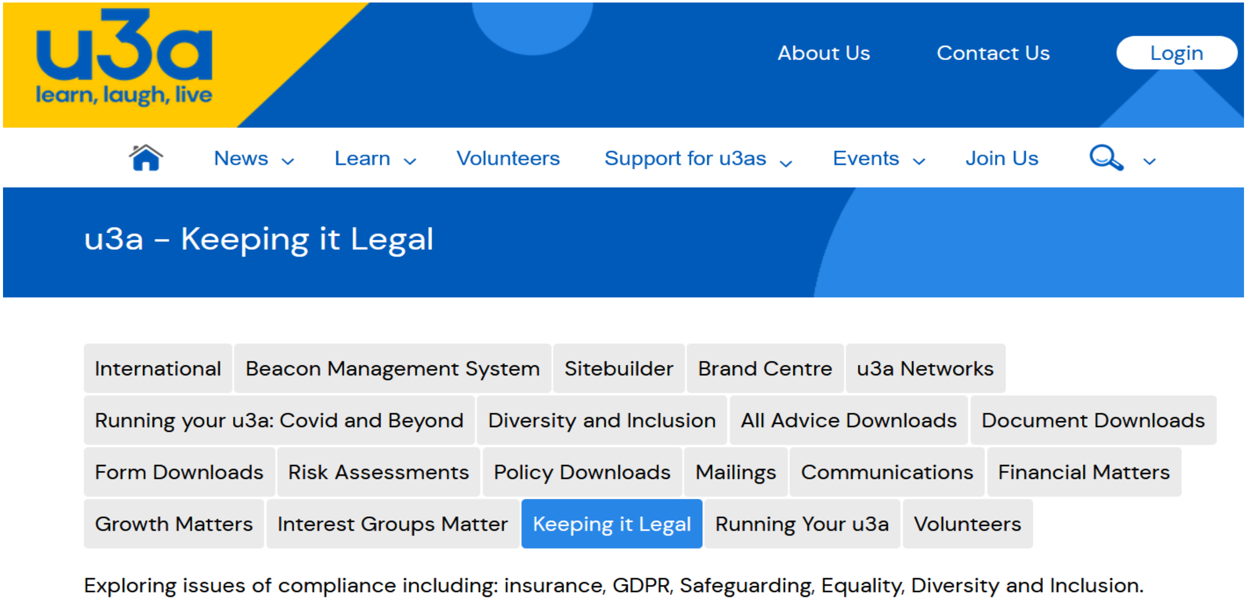
## 8. Data Inventory

It is also important to know where all your U3A's personal data is stored. Consideration should be given of developing a Data Inventory to track, define and record where all personal data is logged.

Appendix 4 has an example. This can become unmanageable but it is a way of realising the breadth of your data storage and the number of locations where data is held. Hence in turn it allows you to consider how this can minimised, whether duplication be eradicated, and if old logs can be deleted.

## 9. Reference Material

The Third Age Trust's 'Support for u3as' section of their website:



u3a – Keeping it Legal

Exploring issues of compliance including: insurance, GDPR, Safeguarding, Equality, Diversity and Inclusion.

The website hosts a specific document on data protection:
https://www.u3a.org.uk/advice/keeping-it-legal/522-data-protection-policy-template-u3a-kms-doc-053

## 10. Contact Point

If you have any comments on this SPG please contact the LRU3A webmaster at:
webmaster.londonregionu3a@gmail.com

**APPENDIX 1 – AUDIT COMPLIANCE CHECKLIST** **DATE …………..** **COMPLETED BY: ----------------------------------------------------**

| REF | SUBJECT DESCRIPTION | ACCEPTANCE LEVEL | STATUS (Yes, No,?, n/a) | NOTES/ACTION | DONE |
|---|---|---|---|---|---|
| **DOCUMENTATION** | | | | | |
| 1a. | **Data Protection Policy** (DPP) created? | Based on template from Third Age Trust (TAT) Website. | | | |
| 1b. | Data Protection Policy up to date? | Needs to be checked at agreed frequency. | | | |
| 2a. | **Privacy Policy** (or Statement) created? | Based on template from TAT Website. | | | |
| 2b. | Privacy Policy (or Statement) up to date? | Needs to be checked at agreed frequency. | | | |
| 2c. | Privacy Policy (or Statement) published to membership? | On u3a's own website or issued to members as part of joining process. | | | |
| 3a. | **Legitimate Interest Agreement** (LIA) created if necessary? | Required if DPP says Legitimate Interest is part of legal basis. Based on template from TAT Website. | | | |
| 3b. | LIA up to date? | Needs to be checked at agreed frequency. | | | |
| 4a. | Is an additional GDPR **Consent Declaration** required for Committee members/other data-users? | Can be seen as clarity & useful protection for Trustees/other data-users and other members processing members' data. Based on template in Appendix 2. | | | |
| 4b. | If so, are Declarations (paper or digital) for each relevant member on file? | Need to be checked at agreed frequency. | | | |
| 5a. | Are there any **other GDPR documents** prepared by your | Consider if any are needed, advice in ~~(See~~ Appendix 3~~.)~~ | | | |

| | | | | | |
|---|---|---|---|---|---|
| | u3a? eg Website/Cookies Policy~~?~~ | | | | |
| 5b. | Are these additional ~~option~~ documents up to date? | Needs to be checked at agreed frequency. | | | |
| | | | | | |
| **SYSTEMS** | | | | | |
| 6a. | Where & how is **members' personal data?** stored? | Consider digital/ paper; current/archive. | | | |
| 6b. | Who has access to this data? | Consider how to minimise this and ensure secure storage. | | | |
| 6c. | What about any **non-members'** data, eg emergency contact, visiting speakers? | Consider any consents required & system for keeping up-to-date. | | | |
| 6d. | Is a **Data Inventory** log utilised? | Consider; see Appendix 4 for an example. | | | |
| 7. | **Handover**: have previous post-holders confirmed they have retained no personal data? | Written record of this confirmation (eg an email on file). | | | |
| 8a. | Is an **Event Management System**: if one is used, is it GDPR compliant? | If so, check it is GDPR compliant. | | | |
| 8b. | Are eg registration records downloaded, are they kept? | If so, check they are deleted periodically. ? | | | |
| 8c. | Who has access to this data source? | Consider how to minimise this | | | |
| 9a. | Is a proprietary **mass mailing system** used (other than Beacon)? | If so, check it is GDPR compliant. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 9b | Are the contact details maintained, ie old contacts removed? How frequently? | If so, check they are deleted periodically. | | | |
| 10. | Is any personal data visible to the public, eg on your **website or publicity materials**? | Check and consider alternative systems. | | | |
| 11. | Are **alias email addresses** used? Who manages? | Consider introducing if not. | | | |
| 12a. | Is a **Cloud Storage System** used? | If so, check it is GDPR compliant. | | | |
| 12b. | How extensive is the Cloud storage, what personal data is stored there? | | | | |
| 13a. | Is **Zoom** or other conferencing system used? | Check the account holder(s) comply with GDPR. | | | |
| 13b. | Are Zoom reports utilised? | Check data is not stored longer than necessary. | | | |
| | | | | | |
| **GENERAL / OTHERS** | | | | | |
| 14. | Do **Group Leaders** understand how to be GDPR-compliant, the need to blind copy emails; safe storage of data (paper & digital)? | Check & offer assistance if needed; encourage only the minimum of data storage. See also section 4 above, GDPR **Consent Declaration**. | | | |
| 15. | Is there a **Data Protection Officer** nominated? | Consider whether to have individual or committee responsibility | | | |
| 16. | Is GDPR covered in **Trustee/ Committee member induction** processes? | Include it if not | | | |

| | | | | | |
|---|---|---|---|---|---|
| 17. | Have any **data breaches** occurred? | If so, consider how they were handled/reported, and modify systems if necessary. | | | |
| | Anything else? | | | | |

## APPENDIX 2 – EXECUTIVE COMMITTEE AND OTHERS - GDPR CONSENT FORM

To ?????? u3a

In addition to any other processing of my personal data that may be permitted under [name of u3a] u3a's Data Protection Policy relating to the processing of personal data, I confirm that, as either a member of the Executive Committee or as a support member, I am happy:

(a) for my name, address, email address and telephone number(s) to be shared for purposes relating to the administration of [name of u3a] with the other members of the Executive Committee and any other persons who may support the workings of the Executive Committee;

(b) for my photograph to be included on the [name of u3a] website or used in other forms of its publicity; and

(c) for any of my above or other personal data to be provided to the Charity Commission and any bank or financial institution with which [name of u3a] has or is applying for an account as may be necessary in order to comply with the Charity Commission's or (as the case may be) such bank's or financial institution's registration, account and other requirements from time to time and for any such personal data to be shared with other members of the Executive Committee or support team.

I understand that I can at any time withdraw this consent by contacting [name of u3a] u3a at:
Email: [email of membership secretary]

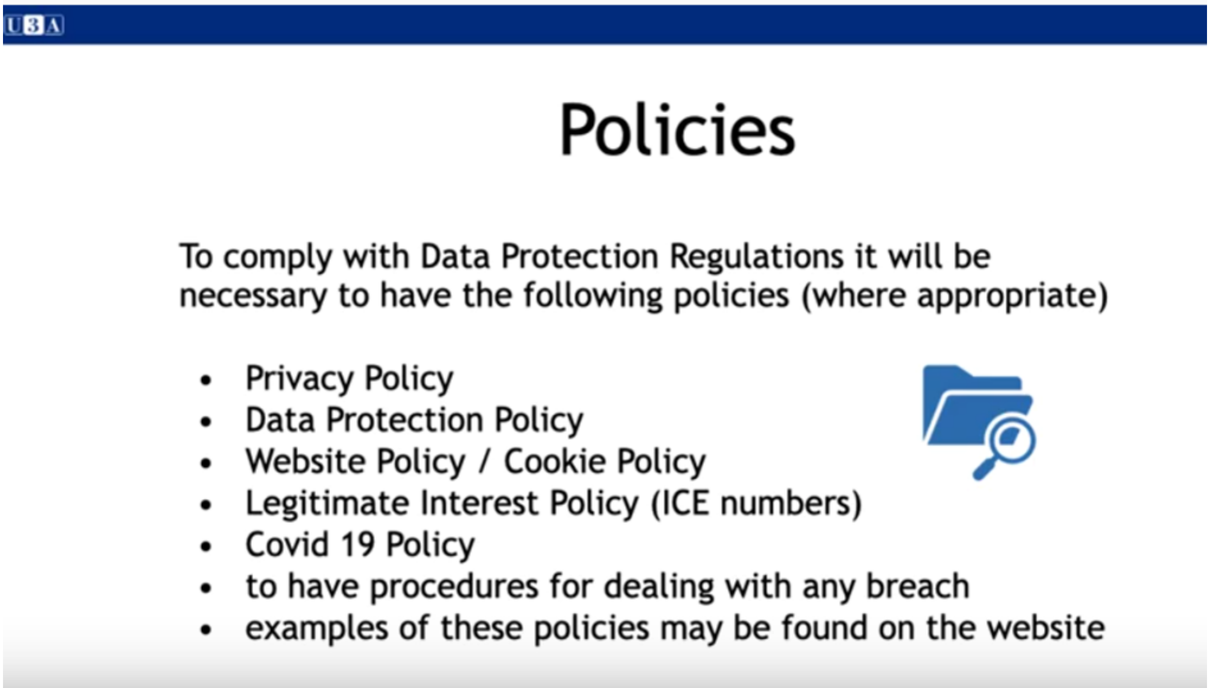
although any such withdrawal will be without prejudice to [name of u3a] u3a's right to continue to hold and process any such data where such holding and processing is permitted by law regardless of my consent.

Signed: ………………………………………………….

Name (print): ……………………………………………..

Date: …………………………………………………..

## APPENDIX 3 – VOLFEST GDPR DOCUMENTATION RECOMMENDATION



### Policies

To comply with Data Protection Regulations it will be necessary to have the following policies (where appropriate)

- Privacy Policy
- Data Protection Policy
- Website Policy / Cookie Policy
- Legitimate Interest Policy (ICE numbers)
- Covid 19 Policy
- to have procedures for dealing with any breach
- examples of these policies may be found on the website

## APPENDIX 4 – DATA INVENTORY

| Description | Provenance | Key Personal Data Type | Additional personal data (content) | Format | Document Type | Storage Location | Security/ Access to data | Retention period | Lawful basis for compliance | Disposal procedures |
|---|---|---|---|---|---|---|---|---|---|---|
| **U3A COMMITTEE/SUB-COMMITTEES** | | | | | | | | | | |
| Email correspondence between Committee participants | U3A committee, Subcommittees, Delegates, Trust & National Office, U3A members, Non-U3A members | Name, email, 'phone, ~~Name of U3A~~ | Possibly | Hardcopy & digital | All types | Personal computers, laptops, smart 'phones | No security | Not specified | Legitimate interest for internal communications | |
| Executive Committee Agenda | U3A committee, Subcommittee | Name, email, ~~Name of U3A~~ | | Hardcopy & digital | Agenda, reports | Personal computers, laptops, smart 'phones | No security/ widely disseminated/on website | Not specified | Legitimate interest for internal communications | |
| Executive Committee Minutes | U3A committee, Subcommittee | Name, email, ~~Name of U3A~~ | | Hardcopy & digital | Minutes | Personal computers, laptops, smart 'phones | No security/ widely disseminated/on website | Not specified | Legitimate interest for internal communications | |
| **DELEGATES/FORUM** | | | | | | | | Not specified | | |
| Delegate/Chair Registration form | Delegates, Chairs | Name, email, 'phone, Name of U3A, position | | | | | **To be determined** | | | |
| Delegate Meeting Agenda | U3A committee, Subcommittee | Name, Name of U3A, ~~possibly~~ email, ~~position~~ | | Hardcopy & digital | Agenda, reports | Personal computers, laptops, smart 'phones, website | Emails disseminated as Bcc/Agenda on website | Not specified | Participation | |
| Delegate Meeting Minutes | U3A committee, Subcommittee | Name, Name of U3A, ~~possibly~~ email, ~~position~~ | | Hardcopy & digital | Agenda, reports | Personal computers, laptops, smart 'phones, website | Emails disseminated as Bcc/Minutes on website | Not specified | Participation | |
| Reports for Delegate Meetings | U3A committee, Subcommittees, Delegates, Local Networks,Trust & National Office, U3A members, Non-U3A members | Name, Name of U3A, ~~possibly~~ email, ~~position~~ | | Hardcopy & digital | Agenda, reports | Personal computers, laptops, smart 'phones, website | Emails disseminated as Bcc/Reports on website | Not specified | Participation | |
| News & information | Anywhere | Name, Name of U3A, ~~possibly~~ email, ~~position~~ | | Digital | All types | Personal computers, laptops, smart 'phones, website | Emails disseminated as Bcc to Delegates for onward dissemination/Information may be on website | Not specified | Participation | |
| **SUMMER SCHOOL APPLICATIONS** | | | | | | | | | | |
| Summer School Bookings | U3A members | Name, email, 'phone, Name of U3A<br>Postal address only if no email available | Possibly Dietary, Access information | Hardcopy postal applications & digital online applications | Form, database, emails | External databases (Wufoo & Paypal) + data can be downloaded and stored on personal computers, laptops, smart 'phones | Password protected access by administrators to external databases. Full access administrators can enter, edit & delete data. Others may be limited to view only. | Should be no more than 12 months unless consent received to use information about future Summer School | Contract | Should delete after 12 months unless consent received to use information about future Summer School |
| Summer School Reports -- Wufoo downloaded reports | U3A members | Name, email, 'phone, Name of U3A<br>Postal address only if no email available | Possibly Dietary, Access information | Digital | Form, database, emails | External databases (Wufoo & Paypal) + data can be downloaded and stored on personal computers, laptops, smart 'phones | Data may be view and shared between administrators | Should be no more than 12 months unless consent received to use information about future Summer School | Contract | Should delete after 12 months unless consent received to use information about future Summer School |
| Summer School Reports -- Paypal downloaded reports | U3A members | Name, payment amount (no other personal or financial details) | Possibly Dietary, Access information | Digital | Database | External databases (Wufoo & Paypal) + data can be downloaded and stored on personal computers, laptops, smart 'phones | Data may be view and shared between administrators | Should be no more than 12 months | Contract | Should delete after 12 months |
| Correspondence with Summer School Applicants | U3A members | Name, email, 'phone, Name of U3A<br>Postal address only if no email available | Possibly Dietary, Access information | Hardcopy & digital | Form, database, emails | External databases (Wufoo & Paypal) + data can be downloaded and stored on personal computers, laptops, smart 'phones | Data may be view and shared between administrators and applicants | Should be no more than 12 months unless consent received to use information about future Summer School | Contract & customer service | Should delete after 12 months unless consent received to use information about future Summer School |
| **OTHER EVENTS** | | | | | | | | | | |
| Online booking systems similar to Summer School (e.g. Research Study Day) | U3A members | Name, email, 'phone, Name of U3A<br>Postal address only if no email available | Possibly Dietary, Access information | Hardcopy & digital | Form, database, emails | External databases (Wufoo & Paypal) + data can be downloaded and stored on personal computers, laptops, smart 'phones | Password protected access by administrators to external databases; can limit permissions view only | Should be no more than 12 months unless consent received to use information about future Summer School | Contract & customer service | Should delete after 12 months unless consent received to use information about future Summer School |
| Manual systems (e.g. Music Day) | U3A members | Name, email, postal address, 'phone, Name of U3A | Possibly Dietary, Access information | Hardcopy & digital | Form, database or spreadsheet, emails | Home computer/laptop | Not specified | Should be no more than 12 months unless consent received to use information about future Summer School | | Should delete after 12 months unless consent received to use information about future Summer School |