GDPR Key Points for Branch Committees

Updated April 2021

This document is designed to assist all STEP Branch Committees with their GDPR EU and also the new GDPR UK commitments, with a summary of key areas that are required for compliance. All branches must comply with these guidelines.

Topics covered include:

- STEP Email Usage
- Data Collection
- Data Storage
- Data Retention
- Email Usage
- Subject Access Requests
- Data Breaches
- Branch Websites
- Article 5 Principles of Data Processing

STEP Email Usage

If you have been assigned a STEP email address, please make sure that:

- STEP has a record of all persons with direct access to the email account
- If any staff changes are made to those who have direct access, this information is made available to STEP
- The login details are not shared with anyone outside of those known users

Data Collection

If your branch collects data (e.g. from event attendees) there are a number of precautionary tasks that must be carried out.

- **Individuals must actively opt-in to any future marketing communications**
  
  If you intend to converse with attendees after the event, you must receive and fully document their consent via an opt-in clause on sign up. If you intend to share their information with third parties, this must be made clear with a separate opt-in option.

- **Record all information**

  If an individual consents to marketing, you must document all information in relation to this. Items recorded must contain the date, location (if obtained at an event) and what personal information was collected.

- **All details collected must be stored securely and kept up to date**

  All non-member data collected should be sent securely to STEP Head Office to be stored on STEP’s central database. This will ensure there is just single record of this information, which enables us to comply with other areas of GDPR such as:
• Opt-out
  Aids us in managing and complying to requests of no further communication

• Subject access requests
  Minimises risk of missing data if a request for all data stored about a subject is received

• Right to erasure
  Minimises risk of retaining personal data when a request for removal has been received

• Photography and video of individuals during events is personal data
If you intend to take pictures or video, individuals must be informed. This can be in the form of a general statement when an individual books an event that photography or video will be taken and may be used in promotional material.

• Uploading to STEP
  STEP have a dedicated sharefile account specifically for uploading personal data. For further details, please contact: Branch.Support@step.org

Data Storage
When storing personal information, special consideration must be taken on how that information is stored. Data should always be stored securely with no exceptions. Important areas are:

• Drive encryption
  Most versions of Microsoft Windows have the ability to encrypt drives. If using a portable computer, this is even more important due to the ease with which such a device can be lost or stolen.

• Never store personal information on portable drives or USB sticks.
Due the very nature of portable hard drives and USB sticks, data should never be stored on such a device. There are no circumstances where this can be considered a legitimate option and must be avoided at all costs.

• Hard copies of personal data
  GDPR also affects printed copies of personal data. When dealing with paper revisions of important information about members, for as long as the information is required (see note on Data Retention below), all copies must be kept in a secure location, such as a lockable cabinet.

• Restricted access
  Only those who have been granted specific access by STEP Head Office should be able to view STEP member data. To aid enforcement:
  
  • Each user should have their own profile on a PC so that each user of the computer can only view their data.
  • If on a shared network, use access control lists (folder permissions).
  • If the data is stored in a Microsoft office format, password protect the file.
  • Keep all hard copies in a locked cabinet.
  • Never share login details for an account that has access to member’s personal information.

• Lock screen
  All versions of windows have the ability to lock the screen after a period of inactivity (via the screen saver). This should be enabled to help protect the data from unwanted
viewing. To lock your screen manually, use CTRL ALT DELETE on your keyboard and select ‘lock this computer’ from the on screen menu.

- **Anti-Virus / Firewall**
  All computers used to store STEP data must have adequate anti-virus protection and firewalls. This will help guard against data theft, corruption, and loss of work.

**Data Retention**

GDPR guidelines are very clear on data retention. Personal information should only be stored for the duration of the task involved. Once this time line has been reached:

- **Unless legally required, all data must be removed and deleted**

  Legal requirements to keep data can take the form of a complaint about a member, if your particular geographical location has specific laws requesting it, or when a financial transaction is involved (The UK’s Company Act states this data should be kept for six years)

- **When legally required to keep the data**

  The data must be stored securely and in such a way that direct access is only available for specific purposes.

- **Destruction of all hard copies**

  If the personal data has been printed at any point, these must be destroyed in an appropriate matter (e.g. shredded, etc)

**Email Usage**

When sending emails on behalf of your committee, there are a number of guidelines to consider. STEP are preparing individual email addresses and mailboxes for each branch, which we are now beginning to roll out. In the interest of email safety, our policy covers the following:

- **Access to email account**

  Please make sure STEP has a record of all persons with direct access to the email account. If at any point there is a change of who has direct access, please make STEP aware as soon as possible.

  Only branch members who have signed a branch agreement can access STEP email and accept data for their relevant area. If the administrator role is vacated and a new person accepts the role, STEP Head Office must be notified with immediate effect. The login details must not be shared with anyone outside of this agreement.

- **Sending member details to other branch recipients**

  Unless there is a business need, you should not email member details to other branches or to anyone who is not a member of your committee. All branches should request their respective branch reports via the STEP Head Office so that the member data is guaranteed to be up to date. For assistance, email Branch.Support@step.org

- **Use BCC**

  To safeguard the personal details of the recipients, when sending emails to more than one individual you should always use the BCC field in the email client.
• **Restricted access to mailbox**

Never grant access to your STEP Branch email account to an unknown source. Mailbox access must be kept private and never shared.

• **Storing emails**

Branch reports and any other spreadsheets or documents containing personal data should not be stored in your email mailbox. This can lead to out of date information being retained, and poses a security risk. Reports should always be deleted when no longer required.

### Subject Access Requests

Individuals have the right to access their personal data. To enable access to personal data and any processing it has been used for, an individual can send a subject access request, or SAR. Individuals can make a subject access request verbally or in writing, so any such request must be accurately recorded and actioned in a specific time limit. If you receive a subject access request against STEP data, STEP Head Office must be informed without delay with full details of the incident.

• **Acknowledge the request**

Once STEP has received a SAR, the details of the request must be recorded. Once the request has been recorded, an acknowledgement must be sent to the data subject explaining this, which triggers the time limit.

Once notification has been sent, there is a limit of one month to respond to a request.

• **Collate all data & processing information**

All personal data held must be collated for compliance. All processing must be recorded and included in the SAR. (Such as sending of emails, how often the data was used for statistics etc.). This will include data and processing conducted by STEP Head Office, and the affected branch.

### Data Breaches

When working with personal information, it is important to understand how to address a data breach. Due to the very nature and severity of the subject, some important areas of concern are:

• **Report all data breaches**

All data breaches, whether suspected or actual must be reported if there is a risk to personal data. Were possible, a breach report should be made within 24 hours of occurrence, or within the regulatory limit of 72 hours. This is a requirement of GDPR.

• **Contact STEP Head Office**

Contact must be made with the STEP data protection team as soon as the breach has been noted. Please email [data.protection@step.org](mailto:data.protection@step.org) with details of what occurred, and what data may be at risk. You will receive a response with the relevant form to fill out that will help us understand the implications, and what further action needs to be taken.
• Collect all possible details of breach
Collect as much information about the breach as possible. So that once you receive the data breach form, you are able to fill out all the listed fields with as much detail as available.

• Severity of breach
Minor breaches may only require basic remedial action, but a more serious occurrence can require vastly more work to rectify and possibly trigger further action from outside of STEP (such as Supervisory Authority or local law enforcement).
Bear in mind all data breaches must be reported irrespective of their suspected severity.

• Types of breach
Data breaches can be, but are not limited to:
  o Email account hacked
  o Website hacked
  o Lost devices such as laptops, iPad, smartphones, or any storage device
  o Errors resulting in personal data being unexpectedly shared (e.g. email recipients CC’d rather than Bcc’d)
  o Missing paper copies of personal data
  o Viral infection on any device (PC, MAC, smartphone)
  o Suspected access to device from unknown persons
  o Office intrusions

Branch Websites
If you manage a branch website that is not hosted or managed by the STEP web team, there are a number of checks that must be completed:

• Does it host members’ data?
If the answer is yes, you must be sure that consent has been obtained and documented. Without this, the information if viewable may breach GDPR. If there are any concerns, you must remove the data or request (and document) consent from the persons in question.

• Is the privacy notice available and up to date?
All websites must contain a link to a privacy notice. This document should be specific in topics covered, easy to follow, and written in such a way that any visitor to the site is able to understand how we manage personal data. For an example, please click the following link: www.step.org/privacy

• Do you have a cookies pop up?
All websites must contain a pop up that alerts a visitor to the use of cookies. By their very nature, cookies gather data about a visitor which can contain personal information. There should be a process in place that enables someone to choose whether or not cookies are active. Pointing the popup to a cookie policy can fulfil this role. Please visit www.step.org for an example of this.

• Do you use certificates (HTTPS) to secure data transfer?
Securing a website with certificates is a good way to ensure the integrity of the data when going from the host to the visitor and vice versa. When a user visits a site, the information is sent to their computer using one of two protocols – HTTP and HTTPS.
When a site is secured with certificates, all data transferred is encrypted making any sort of interception impossible. If you are not sure if your webpage is using this security measure, check to see if when loading it uses HTTP or HTTPS at the beginning of the URL.

- **Is your hosting platform GDPR compliant?**
  All contracts must now contain clauses for GDPR. If you are unsure whether your contract with the hosting company complies, please contact Data.Protection@step.org

- **Are the contact details up to date?**
  It is important a visitor is able to contact you via details found on your site. This information should be included in your data protection notice or separately within a contacts page.

### Article 5

Principles relating to processing of personal data

**Personal data shall be:**

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

If you have any questions, concerns or require further guidance, please contact us.

Data protection queries: Data.Protection@step.org

Branch support queries: Branch.Support@step.org