Scripture Union International

Staff Guidance

Handling Personal Data

Table of Contents

1. Introduction 3
2. Information Governance Structure 4
3. Collection and Use of Personal Data 4
4. Internal Disclosure 5
5. External Disclosures 6
6. Updating Personal Data 7
7. Information Security 7
8. Retention & Secure Destruction 8
9. Data Subjects' Rights 8
10. Personal Data Breaches 9

1. Introduction

The Data Protection Act 2018 ('the DPA') governs the use of personal data by organisations based in the UK. It came into effect on 23rd May 2018 and enacts the EU's standards for protection of personal data as set down in the General Data Protection Regulation ('GDPR'), albeit with some technical adjustments (*"derogations"*) that modify the implementation of the GDPR in the UK.

The DPA sets out rules for governing how SUI can use personal data as an organisation. The purpose of this document is to provide guidance to staff on implementing procedures which support and ensure SUI's compliance with the DPA.

Specifically, the DPA requires that we:

- Only use personal data where we need to and only use the minimum required to achieve our objectives;
- Are transparent about how and why we use personal data;
- Have a lawful basis for using that data;
- Have systems in place for correcting inaccurate personal data and keeping that data up to date;
- Have systems in place to securely destroy data where we no longer need it;
- Apply appropriate security measures which protect personal data; and
- Do not transfer personal data outside the EU unless very specific adequacy arrangements are in place.

Note that the DPA is designed to protect the personal data of *EU citizens*. Accordingly, even if you are working overseas within the wider Scripture Union global community, it is important to recognise that your activities may still be covered by the DPA if you are processing – that is, handling – personal data of an individual if that individual was resident in the EU when the data was collected. This might include, for example, personal addresses of programme funders.

Be aware that under the DPA, *sensitive* personal data is afforded an even higher level of protection. Sensitive personal data is information about an individual's race, ethnicity, commission of a criminal offence (or the fact they have been subject to criminal proceedings), political opinions, religious beliefs and their membership of a trade union.

The DPA is generally much stricter than the preceding legislation – in place since 1998 – in terms of when we can use personal data, what we need to tell individuals about how we use it, and how quickly we need to respond in the event of a personal data breach (see section 9 for further guidance). The criminal offences and heavy financial penalties set down in the GDPR are maintained in the DPA. The DPA also requires us to demonstrate how we comply with the Regulation and introduce stricter fines for non-compliance. You can read more about how SUI has responded to the new guidelines in the SUI Data Protection Policy.

2. Information Governance Structure

SUI's Data Protection Policy sets out in detail how we as an organisation comply with the DPA. All staff are responsible for complying with SUI's Data Protection Policy, and all managers are responsible for ensuring that the staff reporting to them staff follow SUI's Data Protection policies, processes and guidance. In practice, this means that managers should make their staff aware of the Data Protection Policy and, where appropriate, advise staff where and when those processes should be followed. At an Executive level, the Scripture Union International Board similarly carries responsibility for promoting these policies and processes throughout the organisation and is ultimately liable for any breach.

3. Collection and Use of Personal Data

3.1 Data Minimisation

- Consider whether you still need any personal data held to achieve your objective.

For example, you decides to review the efficacy and suitability of its funding channels. you may need to collect personal data from trusts, foundations and donors to undertake this analysis. However, once the data has been analysed and statistics have been prepared it may no longer be necessary to retain the personal data in order to conduct the review. In that case, identifiable information (e.g. donors names and email addresses) should be removed from the statistical information.

- Only collect or use the minimum amount of personal data needed for your specific business objective.

For example, to administer an education grant scheme, you may need to collect individuals' names, addresses and student matriculation numbers, but would not need to collect other types of personal data such as age or ethnicity.

3.2 Transparency

- Ensure individuals have been given information about how and why we use their personal data, how long we hold onto their data, who we share it with, SUI's responsibilities under the DPA, and their rights in relation to their data under that Act ('the fair processing information'). This should be in the form of the SUI Fair Processing Notice, which is available from the International Director.

- If your reason for using personal data isn't addressed in the Fair Processing Notice, contact your manager or the International Director who can arrange for the notice to be updated or advise on alternative methods for communication.
- If you need to provide the Fair Processing Notice for a very specific service or purpose (such as an online survey or a recruitment site), please contact the International Director who will arrange for you to be provided with a bespoke template notice.

4. Internal Disclosure

- Only share personal data with other teams where those teams have a genuine business need to access the personal data.
- Only share the minimum amount of personal data those teams need to deliver their business objective.
- If you plan to share personal data with a team on a routine basis and haven't previously done so, inform the International Director of your intentions. If you or your manager have concerns about sharing the personal data then contact the International Director for advice.
- Ensure that you have implemented a secure method of sharing the personal data between your teams.

For example, if you need to share large volumes of data or sensitive personal data on a regular basis with another team you could establish a shared folder on SUI's own systems. You would need to limit the access to the appropriate individuals.

Alternatively, you could apply the password protect feature to the document containing the personal data. The password should be sent separately from the document.

- If you are the team receiving the personal data, you will need to consider whether individuals have been informed about the intended use of the data (see transparency section above).
- If you are using the data for an entirely new purpose, you should also complete a Privacy Impact Assessment screening to identify whether a Privacy Impact Assessment (PIA) should be undertaken. Contact the International Director for guidance.

5. External Disclosures

5.1 Ad-hoc Disclosures

- Teams may receive a broad range of requests from external organisations to disclose personal data.
- Teams should only disclose personal data to external organisation where they have the individual's consent to do so or where there is another legal basis for doing so.

For example, you may receive a request from police asking for information about a volunteer in the context of a criminal investigation. If you receive such a request please contact the International Director who will oversee the disclosure, reviewing the request to ensure that there is a lawful basis for disclosure and liaising directly with the police.

- If you are satisfied that you have an individual's consent to disclose or there is another alternative legal basis to make the disclosure, then before you disclose the personal data make sure you are confident about the requester's identity.

For example, if you have received a phone call requesting disclosure you could ask the requester from a particular organisation to send an email to verify their identity. You should check the email address to check it is a recognisable address affiliated with that organisation. As a matter of course you should check email addresses are recognisable addresses before disclosing personal data. If you are unsure you must contact the International Director.

5.2 Regular Disclosures

- If you are contracting an external organisation to deliver services on behalf of SUI, you will need to enter into a contract with that organisation insisting upon specific measures such as requiring the contractor to impose appropriate security measures to protect the data.
- If you are sharing personal data on a regular basis with another organisation and you aren't paying that organisation for a service, then it may be necessary to enter into an "information sharing" agreement. An information sharing agreement should always be in place if sharing high volumes of data or data of a particular sensitivity (such as medical information or information about criminal offences). Please speak with the International Director who will advise.
- Each team should maintain a central list of organisations with whom they regularly share personal data including contractors, peer organisations, government bodies, public authorities etc.

- Teams should regularly review these lists (e.g. on a quarterly basis) to assess whether you are sharing with new organisations or whether your existing contracts or agreements with these organisations need to be updated.

6. Updating Personal Data

- Where possible teams should implement procedures that enable individuals to easily and quickly update their personal data where they need to update information such as a change in address.

For example, returning volunteers for an SU camp should be asked to renew their enrolment each year, including completing a questionnaire which asks them to update their contact details if they are no longer current.

- Teams should be clear on individual staff members' responsibilities for updating personal data where data is inaccurate or out of date.

For example, in a sports ministry context – for instance, when registration is required for a programme of recurring seasonal activities - managers may decide that individual project-workers are responsible for updating records where changes in circumstances of participants have been advised.

7. Information Security

- Information left unattended is more likely to be stolen, disposed of in error or disclosed to the wrong person. To help protect information, staff should lock their computer screens when away from their desks to avoid sensitive information being viewed by others.
- Staff should also ensure that all sensitive hard copy paperwork is placed in lockable storage – a locked drawer would be enough - at the end of each working day, or whenever it will be left unattended for any length of time.
- Choose a secure password that meets the industry standards – the longer the better, containing a mix of character types (lowercase letter, uppercase, letter punctuation and numeric). It should be different to your last 12 passwords, and complex but memorable.
- Never share your password with anyone else. If you believe that your password is no longer private to you, please change it immediately and advise your manager you have done so.
- Only store personal data on SUI approved systems and equipment. Ideally, store personal data on SUI's own cloud-based systems (such as DropBox).

- If you intend to use another cloud-based system to store personal data, then you must check that the security controls for that system are adequate. If you are unsure about a system you currently use, please contact the host and establish the standards that are being applied.

8. Retention & Secure Destruction

- Staff will need to determine the retention period that is appropriate for the personal data that they hold, and then keep a record of how long they have been storing each item of personal data. Staff should refer to SUI's Data Protection Policy, which sets the SUI's retention periods it recommends for the types of records it currently holds; if you don't think the personal data you hold is covered in this schedule please contact the International Director and agree an appropriate retention period.
- Heads of teams should make clear to their staff who has responsibility for destroying particular records where the retention period for those records have expired. Heads of Teams should ask staff to report on a regular basis to confirm records have been destroyed within these periods.
- Personal data must be destroyed in a suitably secure manner. Personal data in hard copy records should be disposed of in confidential waste bins. Teams should never dispose of personal data in regular waste bins.
- Emails can be deleted by selecting delete and emptying your deleted items folders. There will be similar functions for deleting electronic records in the SUI's other electronic records storage systems. If you are encountering difficulty with deleting your electronic records, please contact the International Director.
- When procuring new IT systems to hold personal data, staff should consider whether the system can be designed to delete records after a particular retention period has expired. Where procuring new IT systems a Privacy Impact Assessment should be undertaken. This will help identify functional requirements (such as automatic deletion) that can help support Data Protection compliance.

9. Data Subjects' Rights

- Data subjects have a range of rights in relation to their personal data including the rights to access their personal data; to request that personal data be deleted; and to request that SUI stops using their personal data in a particular way (such as a request that the SUI stop sending emails to them).
- If you receive a request from an individual to exercise one the above rights, then you will need to inform the International Director as soon as possible who will advise on and help co-ordinate SUI's response. The information may be held in multiple locations. There are strict timescales for complying with the above rights (40 calendar days is the maximum) so please do not delay in getting in contact.

- When contacting the International Director, please consider whether other teams may have access to an individual's personal data and might need to be informed about such a request.

10. Personal Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Data means information in any form including paper records, emails, faxes etc. Examples of personal data breaches can include forwarding a spreadsheet of volunteer data to an unintended recipient (external or internal), or a theft of sensitive documents left in an unlocked room. Personal breaches must be reported to the International Director immediately; if the theft involves a mobile or IT device appropriate action also should be taken directly with the equipment supplier or communications host.

- If you know or suspect a personal data breach may have occurred contact the International Director, who will ask you for details about the circumstances of the breach, the type of data involved and who that data relates to, and the potential impact on individuals affected.
- SUI must retain a record of all personal data breaches, regardless of the severity; so all breaches – or suspected breaches - must be notified to the International Director. Furthermore, if the rights or freedoms of the subject may be at risk as a result of the breach, then SUI must also report the breach to the regulator, the Information Commissioner's Office, and will be subject to a strict 72-hour timescale in which to do so. SUI can be fined heavily for failure to report within the period.
- Remember the 72-hour timeframe starts from the moment any individual in the organisation discovers that the personal data breach has occurred – not when it has been reported to the International Director.

Scripture Union International

Version: November 2019