Scouting Ireland

GDPR & Your Scout Group

GDPR Guidance for Scout Groups and volunteers in Scouting Ireland

Document Ref: SIDP-04-G
Effective from: September 2018
Owner: Data Protection Team
Reviewed: August 2021
Next Review Date: August 2022

The following document describes some of the practical actions that need to be in place within your Scout Group to ensure compliance with the GDPR. These guidelines are to assist Scout Groups and volunteers to manage personal data; they have access to and process, in the day-to-day runnings of a Scout Group, in line with changes brought about by GDPR.

Specific Actions for Scout Groups

1. Designate Responsibility

The General Data Protection Regulation sees no distinction between the status of data management activities, data processing and collection by the employees and volunteers of Scouting Ireland. Therefore, staff and volunteers collecting and processing data, are all doing so on behalf of Scouting Ireland. Therefore, all Scout Groups must comply with Scouting Irelands' data protection and other relevant policies in order to protect the personal data in the care of Scouting Ireland and to minimise data breaches.

As a result, every Scout Group should identify someone or a group of people to be the Data Protection Coordinator to ensure they are meeting their Data Protection obligations. Their tasks will include identifying and recording the specific locations where data is held in each Scout Group, ensuring that consent is obtained in the appropriate manner and maintained accordingly. Scouting Ireland nationally has a Data Protection Officer available to Scout Groups to provide assistance in relation to any data protection questions, queries or issues. Queries of this nature can be submitted to dataprotection@scouts.ie.

2. Create a Processing Activities Record

As the saying goes, 'You can't manage what you can't measure' and this is especially true regarding Data Protection. It is imperative that each Scout Group understands exactly what personal information it holds (and is responsible for). To ensure this is clear, it is important that every Scout Group makes an inventory or record of processing activities of the personal data that it holds. A template is available on https://www.scouts.ie/Data-Protection/Scout%20Group%20Supports%20-%20GDPR/

Obviously, the primary source of personal information held by a Scout Group is its Membership Management system (database). All registered members' information is stored on Scouting Irelands Membership Management System (pTools) and responsibility for this information is jointly held by Scouting Ireland nationally and locally by the Scout Group.

Specific consideration must also be given to paper membership forms and how these are managed once they have been completed and received by the Scout Group. It is vitally important that any completed forms are stored securely in a specified location and destroyed when no longer required.
The same logic should be applied to any other system or database used to assist a Scout Group when managing its membership. It is OK to use third-party technology supports in this way but careful attention must be paid to how and where data is stored (it must be secure and should be encrypted) and individuals must be informed if a third party is being used to provide a system for this purpose.

Other likely categories of Personal Information held by Scout Groups will include:

- Information required for a membership application
- Weekly and activity attendance lists
- Text or messaging systems
- Email lists or contact groups
- Section lists – adult and youth
- Information captured on group websites

There may also be others, depending on the individual Scout Group, and it is important that each group has a record of all of the Personal Data that it 'controls'.

3. Third Parties

If your group is using a third-party system (Data Processor), the Scout Group is obliged to ensure the third party is GDPR compliant. A contract or agreement relating to data protection responsibilities between the Scout Group and the third party should be in place in order to demonstrate this compliance. Most of the third-party providers of these kinds of systems (online registration, text messaging, etc.) are well aware of GDPR and will be able to give advice on how they are meeting compliance.

A Controller and Processor should enter into a Data Processing Contract which must, at a minimum, contain the following details:

- The subject matter, duration, nature and purpose of the data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed;
- The obligations and rights of the Controller

A Data Processing Contract should also contain the following mandatory provisions:

1. That the Processor will only process personal data received from the Controller on documented instructions of the Controller (unless required by law to process personal data without such instructions) including in respect of international data transfers;
2. That the Processor ensures that any person(s) processing personal data is subject to a duty of confidentiality;
3. That the Processor takes all measures required relating to Security of Processing including but not limited to implementing appropriate technical and organisational measures to protect personal data received from the Controller;
4. That the Processor obtains either a prior specific authorisation or general written authorisation for any sub-processors the Processor may engage to process the personal data received from the Controller. The Processor must further ensure that where a general written authorisation to the Processor engaging sub-processors is obtained, the Controller has the opportunity to object in advance to each individual sub-Processor to be appointed by the Processor;
5. That any sub-processors engaged by the Processor are subject to the same data protection obligations as the Processor and that the Processor remains directly liable to the Controller for the performance of a sub-processor's data protection obligations;
6. That the Processor assists the Controller by appropriate technical and organisational measures to respond to data subject rights requests under the GDPR;
7. That the Processor assists the Controller to ensure its compliance with obligations under the GDPR in relation to security of data processing, notification of data breaches, and data protection impact assessments;
8. That, at the end of the data processing by the Processor, the Processor deletes or returns the personal data received from the Controller; and
9. That the Processor makes available to the Controller all information necessary and that the Processor allows for and contributes to audits conducted by the Controller or a third party on the Controller's behalf.

4. Membership Forms

The sample membership form published in the www.scouts.ie is GDPR compliant. Scout Groups may use this sample membership form as a template in order to ensure compliance. The sample membership form contains a privacy notice which outlines the information which is required to be provided to individuals prior to the collection of their personal data together with appropriate consent mechanisms.

Sample youth membership form is available on https://www.scouts.ie/Data-Protection/Scout%20Group%20Supports%20-%20GDPR/

5. Consent

GDPR is very clear that an individual must be informed of what their personal information is going to be used for, who will have access to it, where it will be stored and how long it will be held for. In certain circumstances, they must give their consent for their data to be used. Consent must be 'freely given, specific, informed and unambiguous'.
Consent cannot be bundled, i.e. "I consent to my information being used to notify me about my order and for marketing". Therefore, separate consent for each purpose must be obtained. Members cannot be forced into consent or unaware that they are giving consent. Obtaining consent requires a positive indication of agreement – it cannot be inferred through silence (not objecting), pre-ticked boxes or inactivity.

Consent must also be verifiable – Data Controllers must be able to demonstrate that consent was given and an audit trail should be maintained

Note: Where paper forms are used to collect personal information (e.g. membership applications), the retention period (how long it's kept for) of the form, or relevant portion of the form, should align with the need to demonstrate consent. Consent is not deemed to be indefinite and should be refreshed at least every two years; therefore the retention period of the form should be maximum two years. If consent is refreshed every year (i.e. a new form signed every year) the retention period for forms should be one year. This practice can also aid in keeping your information as up-to-date as possible, which is also important under the GDPR.

6. Data Breach Process

If unauthorised access to Personal Data occurs or Personal Data is lost or stolen, this **must** be notified to the Data Protection Commissioner within 72 Hours of being identified. This is a requirement for all paper information and all electronic information (unless the data is encrypted or anonymised).
If the breach is likely to cause harm to the individual (Identity Theft or breach of confidentiality) then the individual must also be informed. A procedure to detect, report and investigate data breaches should be in place.

A Data Breach Process is available at https://www.scouts.ie/legal/data-protection. It is imperative that Data Breaches or possible Data Breaches are not ignored in the hope that no one will notice, they must be investigated and reported if necessary. If a Data Breach or suspected Data Breach is identified within a Scout Group, advice on the procedure to follow including any reporting obligations can be obtained from the Scouting Ireland's Data Protection Officer at dataprotection@scouts.ie

Note: The 72-hour deadline for notification to the Data Protection Commissioner applies irrespective of any steps being taken to understand the causes of the breach.

7. Subject Access Requests Process

Subject Access Requests or SARS allow for any member to request a copy of information held about them. This must be provided in paper format or in a standard electronic format within thirty days. It is no longer allowable to charge for responding to SARs.

The Scouting Ireland's Subject Access Request process is available on at https://www.scouts.ie/legal/data-protection .

It is of utmost importance that Subject Access Requests are responded to and dealt with within the allocated time frame. If a Subject Access Request is received by a Scout Group, guidance on the procedure to deal with same can be obtained from the Scouting Ireland's Data Protection Officer at dataprotection@scouts.ie

Note: Maintaining the Processing Activities Record for your Scout Group as outlined above (2) will be a critical enabler for processing Subject Access Requests in a timely manner.

8. Communications

It is critically important that the wishes of individuals regarding communications sent to them are respected. Consent to contact must be recorded and maintained and if an individual has not given consent to receive communications, they must not be contacted unless we have a lawful reason.

Enhancements have been made to Scouting Ireland systems to facilitate compliance with GDPR using technology, including the Scouting Ireland Membership Management system. This allows Scout Groups members to register and update their details online, thus making the management of consent easier for Scout Groups and reducing the number of paper records required.

Scout Groups may also choose to utilise third parties to communicate with members, however, if Scout Groups choose to do so, the steps included above in relation to Third Parties must be adhered to.

Group Messaging/Emailing
Any Group or section sending communications on behalf of Scouting Ireland or using Scouting Irelands volunteers contact details must be aware that the communication must be compliant with GDPR, specifically the seven principles set out in legislation.
Communications sent via email containing several recipients the 'Bcc' ("blind copy") field must be used to prevent the unnecessary disclosure of recipients' email addresses.

Scout Groups, Sections, etc. using group messaging services such as WhatsApp, Messenger, Viber, should ensure the administrator has received prior consent from each individual. This is necessary due to the fact that once an individual is added to a group their phone number (data) is automatically shared with all those within the group.

Emails containing personal/confidential data sent through smartphones, mobile devices, tablets, etc. should be kept to a minimum. Data sent this way should only be sent using secure devices and secure email. Please review and increase, if necessary, the security settings if using email providers such as Gmail/Hotmail/Yahoo to ensure security. File attachments containing personal data sent via email should be encrypted or password protected and the encryption/password then sent in a separate email.

Where personal/confidential data is sent or received on behalf of Scouting Ireland, or where parents are contacted by email, a private email address must be used. A work address or a shared email (e.g. shared family email) should not be used.

9. Secure Storage

All Personal Data held by the Scout Group, whether in paper form or electronic should be stored safely and securely. Paper copies of Personal Data should be stored in locked cabinets and securely shredded once they have fulfilled their purpose. Electronic copies of Personal Data should be password protected and encrypted. All Microsoft products (Word, Excel etc.) can be password protected by clicking 'File' in the top left corner and 'Protect Document'.

Secure Paper

Ensure all files containing personal data are stored in a secure manner e.g. locked away when not in use and not left unattended on a desk at home or in the Scout Group meeting place. They should be transported securely and never left in a car overnight. Scouting Ireland's member records i.e. group lists, contact details, Application and Registration Forms, Activity Consent forms etc., should be kept to a minimum, stored securely and shredded once no longer required or forwarded to National Office as appropriate. Please note that the safety and wellbeing of our youth members is of the highest importance to Scouting Ireland and this should be considered first and foremost when making adaptions for GDPR.

When data collected via paper has been entered into Scouting Ireland's Membership Management System the paper should either be filed and stored securely for as long as necessary or shredded and destroyed in accordance with Scouting Irelands Retention Schedule.

Personal data stored in paper form, including correspondence (containing personal contact details), should not just be thrown away. It should be disposed of correctly, such as shredded before being disposed of.

With regard to data collection for fundraising in the form of ticket selling or 'line selling' the person's name and contact details collected for the purpose of the draw indicates their permission to enter the raffle. However, once the raffle is complete this data should be destroyed securely. It should not be stored or used for any other purpose than it was collected for.

Secure Electronic

It is recommended that for all computers, laptops and mobile devices, the screen should 'lock' after a few minutes of inaction or when left unattended, and only re-activated by keying in a password.
Where personal records are saved on a mobile device or laptop, they should be saved in a secure, password protected folder, never on the main drive or desktop of the device.
Encryption/Password – Membership Management System, computers/mobile devices should be password protected, and access/login codes should not be shared with anyone else including adult volunteers in your Scout Group or anyone outside of it.

Adult volunteers who access the Membership Management System from a shared computer must:

- Have a password-protected user account on the computer, so that browser settings and files are not shared with, or accessible to others.
- Ensure that they log fully out of the account when not in use or when the computer is unattended.

10. Data Destruction

Data, when no longer being used for the purpose it was collected for, should be either archived and stored securely or destroyed in a safe and secure manner. All paper documents should be shredded before being disposed of. Electronic files should be deleted from all devices they are stored on.

	Time Period for Data Retention
Application/Registration Forms	Keep for one year. New ones should be completed each year. These must be stored securely. Destroy after 1 year.
Event / Activity	Attendance list should be archived after an event. If there was an accident, keep anything related. All other records such as consent forms, health forms: destroy after 3 months
Financial Records & Receipts	Keep for 7 years
Attendance Records/Roll Books	Keep for minimum one year

11. Privacy by Design

GDPR seeks to ensure that all significant new processes, initiatives or projects undertaken consider and ensure GDPR compliance from the outset of the project. This requires a Data Protection Impact Assessment to be undertaken to understand the potential impact of that project / initiative on the privacy of individuals in certain circumstances. Scout Groups that are considering projects with 'high risk' processing (i.e. new technology) or installing CCTV should conduct a Data Privacy Impact Assessment by meeting relevant stakeholders, identifying potential privacy issues and agreeing ways to mitigate the risk of issues occurring. A sample Data Protection Processing Activities Record is available at https://www.scouts.ie/legal/data-protection

12. Training

All Scouting Ireland members and members of the Group Council are encouraged to review the content of the GDPR and My Scout Group guidance to familiarise themselves with the requirements of GDPR.

All data protection training will be linked with Scouting Ireland's ordinary training scheme. It will be embedded in the Scouting Ireland Group Leader training programme. In addition, Data Protection awareness will be integrated into the Being A Scouter training module. A higher level of understanding and practical application of data protection will be provided through Group Leader Training and Scout Group Board of Trustees. Also, modules will be made available at the Scouters Conference.

A number of Data Protection workshops will be organised for the coming months. Scout Groups Data Protection coordinators and any other relevant persons are encouraged to attend. Further Information on how to attend these workshops will be shared on the website.

13. Review Access

Access to all Personal Data held by the Scout Group should be reviewed. This is to include all systems utilised by the Scout Group, such as the Membership Management System, IT software and any other systems used. It should also include physical files that contain Personal Data.
Scout Groups should ensure that previous members of the Scout Group do not have access to key systems and data unless their current role within the Scout Group specifically requires such access. Scout Groups should carry out a review of positions which determine access to membership records contained on the Membership Management System. A similar review should be carried out on all other systems that store data the Scout Group may use.

14. If In Doubt, Ask!

Complying with Data Protection legislation and GDPR can be daunting and it will take some time before all Scouting Ireland volunteers are fully comfortable with the changes that the new regulations have brought, There will always be questions regarding specific processes used in Scout Groups and the simple advice is 'if in doubt, please ask'.

Scouting Ireland has provided a Data Protection Team to assist Scout Groups with their data protection obligations. If any queries in relation to data protection arise please email dataprotection@scouts.ie