Scouting Ireland, National Office, Larch Hill, Dublin 16, Ireland.
T: 01 4956300
www.scouts.ie

	Gasóga na hÉireann / Scouting Ireland			
	No.	**Issued**	**Amended**	**Next Review Date**
	SI-DP-G02	09SEPT2025	NA	September 2027
	Category: Data Protection			
	Guidelines on managing Personal Data Breaches			

Related Documents
SI-DP-01 Scouting Ireland Data Protection Policy
SI-DP-03 Scouting Ireland Data Breach Policy
SI-DP-F02 Data Breach Report Template

Revision Schedule		
Revision	**Date**	**Description**
1.0	09SEPT2025	This is the first version of these guidelines

Scouting Ireland, National Office, Larch Hill, Dublin 16, Ireland.
T: 01 4956300
www.scouts.ie

Table of Contents

Scouting Ireland, National Office, Larch Hill, Dublin 16, Ireland.
T: 01 4956300
www.scouts.ie

Guidelines for Handling Personal Data Breaches

See SI-DP-03 Scouting Ireland Data Breach Policy

1.0 Introduction

This document is to provide guidance and templates on how to handle personal data breaches for volunteer-led Scout Groups and any other volunteer who is notified or identifies a personal data breach.

Scout Groups are joint data controllers of members personal data with Scouting Ireland however there is an element of independent data controllership of personal data they collect and store about their members solely for the purpose of their Scout Group examples are photographs, sign in sheets, email / WhatsApp group messages with members / parents / guardians of members and volunteers etc. The Scout Group will be responsible for reporting the data breach to either Scouting Irelands Data Protection Officer and / or directly to the Data Protection Commissioner depending on the data breach type. Most cases will go through Scouting Irelands Data Protection Officer.

The guidelines also apply to any other role across the organisation whether it is a volunteer, staff member or Board member, sub-committees, core teams and any other role which holds a Scouts.ie email address.

As per GDPR Article 4(12) A personal data breach means a breach of security leading to:

- The accidental or unlawful destruction
- Loss
- Alteration
- Unauthorised disclosure of, or
- Access to, personal data transmitted, stored or otherwise processed.

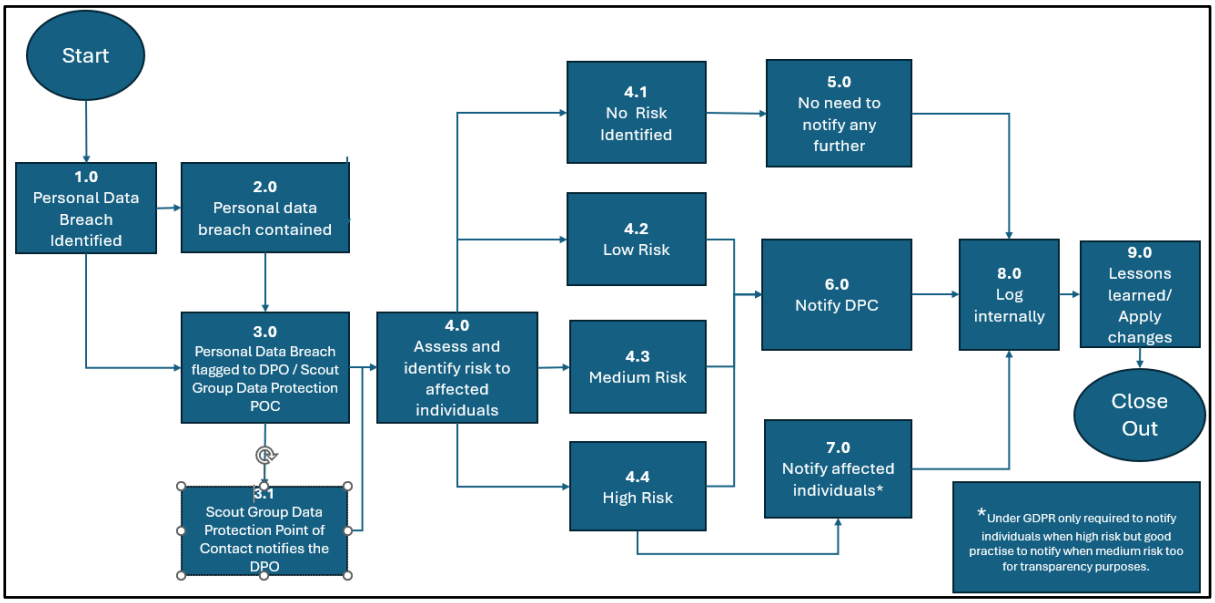
Examples of a **personal data breach** include:

- An email with personal details about a youth member (e.g. medical condition or behavioural information) is sent to the wrong parent
- Disclosure of sensitive personal data without proper authority
- Sending an email to a large number of members / volunteers personal email addresses without using the BCC (Blind Carbon Copy) function
- Paper records with personal or sensitive information are disposed of in a regular bin instead of being shredded
- Paper forms containing personal data, example medication record form or activity consent form left behind on public transport
- Sharing a youth members photograph on social media without parental consent
- A volunteer discussing a member's medical issue or behavioural concerns in a public or inappropriate setting where others can hear.
- Cyberattack or system intrusions where personal data has been compromised

Any questions or for support on how to manage a personal data breach please reach out to Scouting Irelands Data Protection Officer for support (dataprotection@scouts.ie).

It is suggested that one volunteer within a Scout Group is assigned the role of a data protection point of contact. This could be any member of group council it does not have to be the Group Leader.

2.0 Personal Data Breach Process



1.0 Personal Data Breach Identified

A personal data breach can be identified by anyone. Please see section 1 above for examples of personal data breaches.

2.0 Personal Data Breach Contained

Once a personal data breach has been identified, attempts should be made to prevent the personal data from being shared further. Examples are as follows:

- If an email is sent to the wrong person, use the recall function to automatically delete the email from the receiver's account. This only works if recall is an option, and the receiver has not opened the email. Save recall success report.
- If email is sent to an external email i.e. members / volunteers personal email address and / or recall function is not an option, send a follow up email requesting the individual(s) to delete the email (and any copies) immediately and confirm once done. Save the emails where the individual(s) have confirmed deleted.
- Paper records left on public transport – contact the transport provider as soon as possible to report the lost documents and check if they've been found. Keep a record of when you contacted them.
- Accidental sharing of personal data via WhatsApp – select the "delete for everyone" option to delete the message and ask anyone who received the data not to share further and if they saved a copy to delete it immediately.

- Sharing a person's photograph to social media without the correct consent, delete immediately.

3.0 Personal Data Breach flagged to DPO / Data Protection Point of contact.

National level personal data breach report it to Scouting Irelands Data Protection Officer (dataprotection@scouts.ie) immediately.

If a personal data breach occurs at Scout Group level notify your Scout group's data protection point of contact, if this is not known notify your group leader. The Data protection point of contact / group leader should then notify the Data Protection Officer (dataprotection@scouts.ie) for guidance and support as well as tracking purposes. The DPO can help determine if the data breach needs to be reported to the DPC and who is responsible for notifying the DPC.

Please note that containing the data and notifying the relevant person should be done in quick succession of one another. Do not wait until the data is contained to notify the relevant person.

4.0 Assess and identify risk to affected individuals

To decide whether a personal data breach needs to be reported to the Data Protection Commissioner (DPC), affected individuals need to be informed or if it requires internal tracking only, a **risk assessment must be carried out**.

Scouting Irelands Data Protection Officer can provide support and guidance on this. A data breach report template is available to help identify risk and record the necessary details – see **Data Breach Report Template SI-DP-F01**. Please complete this report for each personal data breach.

All data breaches—regardless of severity—should be reported to **Scouting Ireland's Data Protection Officer (DPO)** and **tracked within the Scout Group**. This helps:

- Identify patterns or recurring issues
- Share lessons learned
- Improve data protection practices across the organisation / Scout Group

See DPC Guidance on Risk assessment Data Breach Notification_Practical Guidance_Oct19.pdf

As per the DPC's website:

- **Low Risk:** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- **Medium Risk:** The breach may have an impact on individuals, but the impact is unlikely to be substantial.
- **High Risk:** The breach may have a considerable impact on affected individuals.
- **Severe Risk:** The breach may have a critical, extensive, or dangerous impact on affected individuals.

1. **No Risk identified**? No Notification Needed

If a personal data breach occurs but there is no risk to individuals, you do not need to notify the Data Protection Commissioner (DPC).

However, the incident should still be:

- Recorded internally
- Preventative measures put in place to avoid it happening again
- Lessons learned shared with the relevant team
- Shared with Scouting Irelands Data Protection Officer

2. **Low, Medium, or High / Severe Risk**? Report It

If the breach involves low, medium, or high / severe risk to individuals' personal data, it must be reported to the DPC within 72 hours (GDPR Article 33 (1)) of being made aware of the breach occurring.

3. **Informing Affected Individuals**

As per GDPR Article 34 (1) If the risk is high / severe, you must notify the individuals affected without delay.
If the risk is medium, it is best practice to inform them, even though it's not legally required. This helps maintain transparency and trust with our members.

5.0 No notification required

As above if no risk is identified then no need to notify the DPC or affected individual(s). However please track internally and send on to Scouting Irelands Data Protection Officer (dataprotection@scouts.ie) so they can identify trends across the organisation etc.

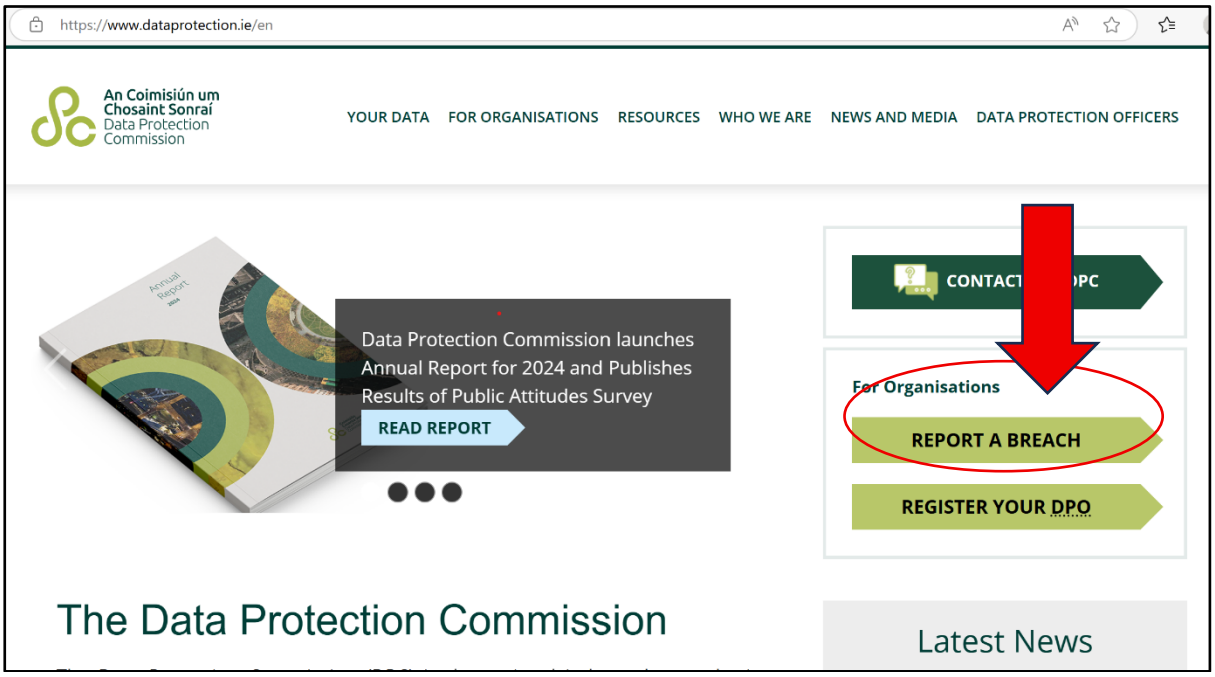
6.0 Notify the Data Protection Commissioner (DPC)

If a low, medium, or high risk is identified, the DPC must be notified within 72 hours. This is regardless of when the data breach happened. Example if you have been made aware of a personal data breach on Thursday at 6pm you have until Sunday 6pm to notify the DPC.

If the breach occurs at Scout Group level and is related to personal data which the Scout group are independent data controller of then this would be reported directly to the DPC by the Scout Group, if it is related to shared data then Scouting Irelands DPO will report the breach to the DPC.

If it is related to Personal data controlled by National office, then Scouting Irelands DPO will report directly to the DPC.

Go to the Data Protection Commissioners website (www.dataprotection.ie) on the homepage there is an option to Report a Breach (circled in the screenshot below).



This will launch a questionnaire – this must be **completed in one go;** you **cannot save** the questionnaire and complete it later. Anything you do not know at the time of completion you can mark this as unknown or provide a best estimate and submit later on. You can do this by going to the report a breach button and select the option to provide an update.

Once completed please ensure you **download a copy** of the report and save it for your records.

7.0 Notify affected individuals

If the personal data breach could potentially be a high risk to the affected individuals then they should be notified as soon as possible. Notification can be via email (if emailing multiple people at once please ensure you use the BCC function). The notification should contain the following:

- A description of the data breach
- The name and contact details of the data protection officer or other data protection point of contact;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Although only legally required to notify affected individuals of a high-risk data breach for transparency purposes and to maintain trust with our members, it is good practice to also notify them of a medium breach too.

8.0 Log Internally

Every personal data breach should be logged regardless of whether it is reported to the DPC and / or individuals, and the following information is included in the tracker:

- Date of Breach
- Incident Description
- Affected Data i.e. First name, last name, email address
- Number of affected individuals
- Notified affected individuals Yes / No and date
- Risk Assessment result i.e. no risk, low / medium / high risk
- Mitigation Measures (Describe the immediate actions taken to mitigate the breach)
- Notified Scouting Irelands DPO? Yes / No and date
- Notification timeline to the DPC (if applicable)
- Remediation Steps (Outline the steps taken to prevent a recurrence of the breach)
- Lessons Learned
- Actions
- Status (Open / Closed)

9.0 Lessons Learned / Record keeping

Identify lessons learned from the personal data breach and apply any identified changes as needed.

Ensure the Data Breach Report Template SI-DP-F02 has been fully completed including the close out summary in the last section of the report.

Save all documentation relating to the data breach, from the initial notice of the breach, any communications you send out to affected parties, the completed DPC report (if applicable) and so on. This should be retained for six years to allow time for affected individuals to raise a complaint or make a legal claim, and ensure we have the necessary information to demonstrate compliance.

3.0 Key Points

- If you are unsure of who to report a personal data breach to reach out to Scouting Irelands Data Protection officer (dataprotection@scouts.ie or 01495 6300).

- If you are a volunteer within a Scout Group and have been made aware of a personal data breach and require support, please do not hesitate to contact Scouting Irelands Data Protection Officer (same details as above). Remember depending on the type of breach it may need to be reported by Scouting Irelands DPO to the Data Protection Commission (DPC) rather than the Scout Group to the DPC.

- Reminder, we have 72 hours to report a personal data breach to the Data Protection Commission if the breach has the potential to cause low, medium or high risk to the affected individuals.

- Affected individuals must be notified if there is a high-risk breach, however for transparency purposes and maintaining trust with our members it is advisable we notify them of medium risk breaches.

- Maintain a data breach log regardless of the outcome and apply lessons learned across the Scout Group.

- Complete the Data Breach Report Template SI-DP-F02 including close out summary.

- Create a data breach package including all documentation around the breach from the initial notice, communications sent out, DPC notice etc. Retain for 6 years from the date the breach occurs.

4.0 SI Data Protection Officer Contact Details

Below are the contact details of Scouting Irelands Data Protection Officer (DPO).

Email: dataprotection@scouts.ie
Phone: 01 495 6300
Address:
Scouting Ireland
National Office
Larch Hill
Dublin
D16 PO23