

Factsheet:

55: GDPR and Data Protection

Last updated: July 2025

Last reviewed: July 2025

1. Outline

This factsheet provides a brief explanation of the responsibilities relating to personal data and data protection that apply to all members of any SSAGO committee, be it Team Pink, club committees or event committees. In all roles, you may be given access to the personal data of SSAGO members, of which SSAGO has a responsibility to safeguard under the law.

2. SSAGO and GDPR

Personal data is defined as information that is related to a specific individual, irrespective of if it could be used to directly identify them or not.¹ By virtue of storing and using this data, SSAGO is considered to be “processing” it, and accordingly is restricted on what we can and cannot do with it, and how we must treat it.

Personal data is considered to be information such as people’s name, contact information, university information and Scouting/Guiding affiliation. Additionally, GDPR defines special categories of personal data that require additional protection² - which, notably for SSAGO, includes health data such as that provided to us on InTouch forms.

As an organisation that collects this data, SSAGO is considered a data controller under GDPR. We must, therefore:

- be upfront and transparent about how we process data and we must not so do beyond what we have stated in [the privacy policy](#);
- keep the data we hold up-to-date;
- dispose of data we no longer need;
- ensure the data we hold is securely stored and take measures to prevent it from being lost or accessed by those who are not authorised to do so.

3. Appropriate Usage

It is only acceptable to use and access the personal data that people have provided to SSAGO in order to deliver events as part of SSAGO (be that nationally or locally). This could include things like contacting people in emergencies or using health information for first

1: [What is personal information: a guide | ICO](#)

2: [What is special category data? | ICO](#)

aid or arranging catering provisions.

If there is any doubt around if you are allowed to do something with a given members' data, you should ask them for permission first. This is especially true if it will involve sharing or distributing data - for example, if you would like to share the phone numbers of first aiders for a camp, you should ensure you have their permission beforehand.

If you make a copy of personal data (e.g. printing InTouch forms, downloading spreadsheets), you should ensure that you do not retain it for any longer than is required. Printed copies should be shredded as soon as possible, and data that needs to be stored long-term should be stored on the SSAGO Google Drive or equivalent Club-managed storage service and not on personal devices or storage services.

You should never access personal data without a legitimate reason to do so, and you should never share it with people who do not need it.

4. Data Breaches

If you become aware of, or suspect, a data breach that has taken place, you should contact Team Pink at pink@ssago.org as soon as possible, detailing:

- What data was lost
- What happened
- When this happened
- When you became aware of the data breach
- Who was involved

You do not need to tell anyone that you have reported a data breach to Team Pink, and you do not need to necessarily be involved in a breach to report one that you have seen.

If a breach involves a member of Team Pink, another, uninvolved member of Team Pink may be informed instead.

On receipt of a notification of a data breach, Team Pink will consider the information provided and respond with a request for further information or any next steps, which could range from no action to a warning for minor or accidental breaches or disciplinary action in serious cases.