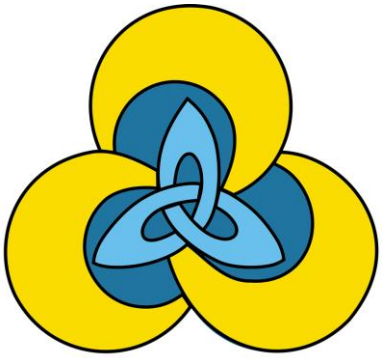

Irish Girl Guides Data Protection Policy

Effective from: December 2014
Designated person responsible: Safeguarding Officer.
Updated August 2019
Overall responsibility: IGG's Executive committee
Last reviewed in: June 2020
To be reviewed in: June 2022

Irish Girl Guides Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the data protection obligations of Irish Girl Guides (IGG). This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish and European legislation, as listed below;

- the General Data Protection Regulation (GDPR) 2018
- the Data Protection Act 2018
- the EC Electronic Communications (2011)

Irish Girl Guides' policies and related statements provide a structure in which Guiding can take place safely, consistently and in accordance with legislation. Policies must be followed by IGG members, staff and recognised volunteers involved in delivering or supporting Guiding.

Rationale

Under the Irish Data Protection legislation, everyone has rights with regard to how their personal information is handled. In order to fulfil its mission, Irish Girl Guides may collect, store and process personal information about members, volunteers, staff, service providers and suppliers.

IGG, as the Data Controller with responsibility for the management of personal data by its members and staff, recognises the need to treat this data in an appropriate and lawful way and is committed to doing so.

Scope

The policy covers both personal and sensitive personal data held in relation to Data Subjects by IGG. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

IGG as a Data Controller

In the course of its daily organisational activities, IGG acquires, processes and stores personal data of individuals, including:

- employees of IGG
- adult members of IGG
- youth members of IGG, their parents and/or guardians
- volunteers working on behalf of IGG
- third party service providers engaged by IGG

Due to the nature of the organisation, there is a regular and active exchange of personal data between IGG and its members. This policy provides the guidelines for this exchange of information, as well as the procedures to follow in the event that an IGG staff member / volunteer is unsure whether such data can be disclosed.

In general terms, the staff member / volunteer should consult with the organisation's Data Protection Officer to seek clarification. It is intended that by complying with these guidelines, IGG will adhere to best practice regarding the applicable Data Protection legislation.

Responsibility for ensuring personal data is processed in accordance with Data Protection regulations lie with the Data Controller i.e. Irish Girl Guides and/or Data Processor i.e. 3rd party processors. While IGG has ultimate responsibility for compliance, all those who collect and process personal data on behalf of IGG i.e. staff and volunteers need to be aware of their responsibilities.

The Data Protection regulation makes no distinction between the status of the data management activities of the employees and the processing activities of volunteers. Therefore, staff and volunteers who gather and process personal data, are doing so on behalf of IGG, and must comply with IGG's data management policies and general policies on confidentiality in order to protect IGG's reputation and to avoid breaches.

Data Protection Principles under GDPR

When processing personal data, IGG in its capacity as Data Controller ensures that all personal data shall comply with all the following principles (the first six being in-line with the previous Data Protection directives)

1. Lawfulness, fairness and transparency – Personal data must be processed lawfully, fairly and in a transparent manner.
2. Purpose Limitation - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation – Personal Data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.
4. Accuracy – Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted.
5. Retention – Personal data should be kept in an identifiable format for no longer than is necessary.
6. Integrity and confidentiality – Personal data should be kept secure.
7. Accountability – An important change for Data Controllers. Under the GDPR, organisations must not only comply with the above six general principles but must be able to demonstrate that they comply by documenting and keeping records of all decisions.

Subject "Access Requests"

IGG has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Any valid, written request by an IGG member or staff for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the IGG Data Protection Officer. Information will be provided without delay and within a month.

Where requests are complex or numerous, under GDPR organisations are permitted to extend the deadline to three months. However, IGG will still respond to the request within a month to explain why the extension is necessary.

Third-Party Processors

In the course of its role as Data Controller, Irish Girl Guides engages with Online Guide Manager and other service providers in order to process Personal Data on its behalf.

In such cases, a formal, written contract will be in place between IGG and the Data Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the applicable Data Protection legislation.

Records Retention and Destruction

IGG are required to retain certain records, usually for a specific amount of time. IGG must balance these requirements with statutory obligations to only keep records for the period required and to comply with data minimisation principles.

IGG have Data Retention and Destruction Policies in place in line with these which must be followed by staff and volunteers. It should be noted that retention obligations apply equally to electronic and paper-based records.

These policies serve to inform all staff members and volunteers who process personal data on behalf of this organisation of the appropriate retention periods for such data. Where relevant, the document identifies relevant legislation. However, Irish Girl Guides may choose to retain data for longer than stipulated in the legislation, where this data supports operational or logistical purposes, to provide administrative services, to meet legal and regulatory requirements or maintain a historical archive of the organisation.

Data Breach Management

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.

In the unfortunate event that there is a data protection breach and personal data is lost or inadvertently disclosed, it is important that IGG's Data Protection Officer (DPO), National Office is informed immediately. The DPO will do everything possible to;

- discover what happened
- put a plan in place to prevent a recurrence
- ensure that organisation's Executive committee, Leaders, volunteers and staff are made aware of any resulting changes in procedure
- log the breach, decisions made and actions taken

IGG's Data Protection Officer must notify the Data Protection Commissioner within 72 hours of becoming aware of a breach, except where the breach has been assessed as unlikely to present any risk to the rights and freedoms of data subjects.

All breaches, even those that are not notified to the Data Protection Commissioner on the basis that they have been assessed as being unlikely to result in a risk, must be recorded, at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response.

IGG is obliged to communicate to the data subject a personal data breach without undue delay, where that personal data breach is likely to result in a high risk to the data subject.

There are, however, circumstances where controllers may not be required to communicate information relating to a data breach to data subjects, even where the breach may be likely to result in a high risk to the rights and freedoms of the natural person. These circumstances are where any of the following conditions are met:

a) The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
c) It would involve disproportionate effort. In such a case, however, controllers must still ensure, by way of a public communication or similar measure that the data subjects are informed in an equally effective manner.