Data Protection - GDPR

Data Protection is a complex area and we are all involved one way or another. In the context of our Scouting lives, the organisation holds records on us at National level and also at Scout Group level. The national organisation (Scouting Ireland Services CLG) is a Data Controller and every Scout Group is also a Data Controller. Indeed it seems likely that the national organisation and each Scout Group are joint controllers of at least some data , such as the membership records. This article aims to shed some light on the subject. It has been produced following a reading of available materials and a consideration of how these apply to Scouting on this island. It should be noted that the author is not an expert in GDPR and anyone concerned about this area should seek appropriate professional advice on the matter.

What is Data Protection

dataprotection.ie

Data protection is a fundamental right set out in Article 8 of the EU Charter of Fundamental Rights, which states;

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

This means that every individual is entitled to have their personal information protected, used in a fair and legal way, and made available to them when they ask for a copy. If an individual feels that their personal information is wrong, they are entitled to ask for that information to be corrected.

What is GDPR

gdpr.eu

The General Data Protection Regulation is a European Union law that was implemented May 25, 2018, and requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. The regulation includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines. The GDPR replaced the 1995 Data Protection Directive, which created a country-by-country patchwork of data protection laws.

Though it was drafted and passed by the European Union, it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.

enterprise.gov.ie

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation on data protection and privacy for individuals within the European Union (EU). The regulation was put into effect on May 25, 2018. As an EU Regulation, the GDPR does not generally require transposition into national law, as EU Regulations have “direct effect”.

Southern Ireland Law

Data Protection - GDPR

The current, relevant legislation in the South of Ireland is the Data Protection Act 2018 which was signed into law on 24 May 2018. Among its provisions, the Act gives further effect to the GDPR in areas where Member States have some flexibility (Part 3 of the Act), for example, the digital age of consent. The legislation confers rights on individuals in relation to the privacy of their personal data as well as responsibilities on those persons holding and processing such data.

UK / Northern Ireland Law

niassembly.gov.uk

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 together form a framework for regulating the processing of personal data in the UK since 25 May 2018, replacing the former Data Protection Act 1998.

What is Personal Data

ec.europa.eu

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.

Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The GDPR protects personal data regardless of the technology used for processing that data - it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored - in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

This link provides further clarification as to what exactly is meant by the term Personal Data. *Article 29 Working Party Opinion 4/2007 on the concept of personal data*

The Opinion sets out that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual.

In order to consider that the data "relate" to an individual, a "content" element OR a "purpose" element OR a "result" element should be present.

- The "content" element is present in those cases where information is given about a particular person, regardless of any purpose on the side of the data controller or of a third party, or the impact of that information on the data subject. Information "relates" to a person when it is "about" that person...
- A "purpose" element can be responsible for the fact that information "relates" to a certain person. That "purpose" element can be considered to exist when the data are used or are likely to be used to evaluate, treat in a certain way or influence the status or behaviour of an individual.

- A third kind of “relating” to specific persons arises when a "result" element is present. Despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It should be noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.

As regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be “identifiable” because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others.

Rights to Access

The General Data Protection Regulation (GDPR), under Article 15, gives individuals the right to request a copy of any of their personal data which are being “processed” (i.e. used in any way) by “controllers” (i.e. those who decide how and why data are processed), as well as other relevant information (as detailed below). These requests are often referred to as “data subject access requests”, or “access requests”.

These requests must be responded to free of charge and in an accessible form, and controllers should seek to facilitate access requests being both made and responded to easily, including electronically where appropriate and where the individual wishes.

The guidance at this link *dataprotection.ie* should answer some of the most frequently asked questions by both individuals who are seeking copies of their personal data, as well as controllers who are struggling to deal with the access requests they are receiving.

This one nicva.org gives information re. Subject Access Requests in Northern Ireland.

From this guidance the following is particularly worth noting:

Are there any other limitations on the right of access?

Under Article 12(5) GDPR, in limited circumstances, where an access request is “manifestly unfounded or excessive”, a controller may also, where appropriate, refuse to act on the request. This is, however, a high threshold to meet, and the controller must be able to prove that the request was manifestly unfounded or excessive, in particular taking into account whether the request is repetitive. There should be very few cases where a controller can justify a refusal of a request on this basis.

There is a general limitation on the exercise of the right of access under Article 15(4) GDPR, which states that the right to obtain a copy of the personal data undergoing processing should not negatively impact (“adversely affect”) the rights and freedoms of others, such as privacy, trade secrets, or intellectual property rights. However, where a controller does have concerns about the impact of complying with a request, their response should not simply be a refusal to provide all information to the individual, but to endeavour to comply with the request insofar as possible whilst ensuring adequate protection for the rights and freedoms of others.

Whilst the right of access to personal data is a fundamental data protection right it is not an absolute one, and is subject to a number of limited exceptions. Article 23 GDPR allows for data subject rights to be restricted in certain circumstances. Any such restrictions must be set out in a "legislative measure", respect the essence of the fundamental rights and freedoms, be necessary and proportionate in a democratic society, and safeguard an interest of public importance.

Accordingly, if a controller considers that it is justified in withholding certain information in response to an access request it must identify an exemption under the GDPR or the relevant Act, provide an explanation as to why it applies, and demonstrate that reliance on the exemption is necessary and proportionate.

Responsible Authorities

Southern Ireland *dataprotection.ie*

The Data Protection Commission (DPC) is the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. The DPC is the Irish supervisory authority for the General Data Protection Regulation (GDPR), and also has functions and powers related to other important regulatory frameworks including the Irish ePrivacy Regulations (2011) and the EU Directive known as the Law Enforcement Directive.

UK / Northern Ireland *ico.org.uk*

The Information Commissioners Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

European Data Protection Board *edpb.europa.eu*

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities. They replaced the Article 29 Working Party when GDPR was put into effect on May 25, 2018.

Information

CitizensInformation.ie

Northern Ireland Council for Voluntary Action

gdpr.eu

tableau.com

Enforcement Trends

arthurcox.com

itgovernance.eu