GDPR Guidance for Irish in Britain Members

This guide is for Irish in Britain Members who are unsure of how the General Data Protection Regulation (GDPR) may affect their organisation. It covers some of the key terms in the GDPR and identifies the changes that are most likely to impact members. The information provided will not be applicable in all cases and you should conduct your own research to ensure that your organisation is compliant with the GDPR's requirements. If you are unsure of what you need to do to prepare for the GDPR, please consult the ICO's website, or contact their helpline for small organisations. This document does not constitute legal advice and should not be construed as legal advice or a legal opinion on any specific facts or circumstances.

Who does it affect?

The GDPR will impact almost every organization in the U.K. in some way. If you have members, run a welfare service, or have a list of regular lunch-club attendees, you may need to change how you collect and handle an individual's information. The GDPR will be enforced from May 25th, 2018.

Terms to know

The GDPR uses a number of different terms to describe the legal requirements for organisations. These terms are often abstract and confusing, so it is important that you have a good grasp of what is being referred to in the legislation.

Controller: The entity that determines the purposes and means of processing personal data (your organisation in most cases).

Processor: The entity responsible for processing personal data on behalf of a controller (a third-party organisation in most cases, e.g., an email marketing company.)

Data subject: An individual whose data you collect and retain, such as a member or newsletter recipient.

Personal Data: Any info relating to an identified or identifiable person including: name, address, mobile number, birth date, etc.

Consent: Direct approval from the data subject (e.g., service user/member or someone who receives a newsletter). One of the most popular means by which an individual's data may be processed.

Legitimate Interest: One of the most popular means by which an individual's data may be processed. Processing an individual's data is necessary for an organisation's interests.

Key Changes

1) Enhanced Consent Collection

Consent must be freely given, specific, and informed. Ensure that anytime you seek consent, whether for a newsletter, membership, activity, etc., you include:

- **Active Opt-in:** Pre-ticked opt-in boxes are invalid. Organisations must use unticked opt-in boxes or similar active opt-in methods (e.g., Select either: Yes, I would like to receive email updates/ No, I would not like to receive email updates).
- **Unbundled**: Consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
- **Granular**: Give options to consent for different types of processing wherever appropriate (e.g., Indicate by which methods you would like to receive updates: phone, email, post.)
- **Named**: Name your organisation and any third-parties who will be relying on the given consent.
- **Easy to Withdraw**: You must tell people they have the right to withdraw their consent at any time and how to do this. It must be as easy to withdraw as it was to give.

The GDPR does not "grandfather" consent. If consent was obtained prior to May 25th, 2018 in a way that does not conform with the GDPR, consent will need to be re-obtained.

Consent must be up-to-date and valid. It is good practice to renew consent every two years.

If you receive consent to send a newsletter, you cannot also send a request for donations unless you have obtained a separate consent. Consent only applies to the specific activity(ies) for which it was requested.

Consent must be recorded when it is obtained and evidence that consent was given must be available if requested. In most cases, a double opt-in procedure is desirable, where a data subject is asked to confirm their consent. A double opt-in procedure may mean a confirmation email sent to an individual who signed up for a newsletter to guarantee against the possibility that their email was submitted without their knowledge.

If information is passed on to a third party with the individual's consent, it is the controller's responsibility to ensure that the third party is made aware of any changes to that information. If an individual would like to modify their information or withdraw consent, then everyone with access to that information must be made aware.

2) Legitimate Interests

An organisation may process an individual's data without obtaining their consent if it is within the legitimate interests of the organisation. Legitimate interest should only be used as the means for processing data on the successful outcome of a Legitimate Interest Assessment (LIA). To complete an LIA, you must identify the legitimate interest, identify why processing is necessary for that interest, and

perform a balancing test. A balancing test weighs a data subject's right to privacy against the organisation's interests and must account for: the nature of the controller's interests, impact on the data subject, how data is processed, reasonable expectations of the data subject, and whether less invasive means may achieve the same result. You will need to keep a record of your LIA and the outcome.

If using legitimate interests as a reason for processing an individual's data, you must:

- Inform the data subject of the purpose of the processing and the legitimate interest you are relying on to process the data at the time of the collection.
- Document and retain the results of the balancing test.
- Inform the data subject that they have the right to object.

“Example Irish Association uses legitimate interests as the basis for maintaining their member’s accounts and performing administrative activities, such as recording attendance at lunch clubs and sign up for events, updating contact information, and contacting them for membership renewal.

They do not use legitimate interests as the basis for contacting members about promotions or events as it did not pass their Legitimate Interest Assessment. They determined that their members’ right to privacy outweighed the organisation’s interests in promoting their activities. Instead, they rely on consent to promote their activities and events.”

3) Increased Transparency

All information must be presented to data subjects in a "concise, transparent, intelligible and easily accessible form, using clear and plain language." When collecting data directly, you must inform data subjects of:

- The controller's identity (your organisation) and contact information
- The Data Protection Officer's contact information (if applicable)
- The purposes and legal basis for processing (e.g., legitimate interest)
- What the legitimate interests of the controller are (if basis on which the controller is relying for processing)
- Who the recipients of the personal data are
- Any intended transfer to a non-EU country and the legal basis of the transfer
- How long data will be stored
- Data subject rights (Right to object, right to withdraw consent)
- How to withdraw consent (if relying on consent for processing)

"*Example Irish Association (EIA) will manage your personal data in accordance with the General Data Protection Regulation, under the basis of legitimate interests. It is in our interests to manage your account in order to update your contact information and record your use of our services, and to contact you to determine if you wish to continue your membership beyond the year. We will only use your supplied information to manage your account and contact you about renewing your membership unless you have consented to be contacted for other purposes. The information you provide will be held for two years, unless you renew your membership, or object to the retention of your data.*

We will contact you regarding events, promotions, and news only if you have consented to this. You may withdraw this consent at any time by contacting EIA directly. Your information will not be transferred to any-third parties or used by anyone not directly affiliated with Example Irish Association. You may object to our retention and processing of your data at any time to a supervisory authority (ICO in the UK). See our full privacy policy for further details."

4) Record Keeping & Notification

Controllers must demonstrate their compliance with the GDPR when requested and must keep a record of their activities and the legal basis under which they are conducted. You must keep a record of your Legitimate Interest Assessment if you are relying on legitimate interest or a record of every instance of given consent if you are relying on consent. You must keep track of who has given you consent, for what, and when they gave it. Consent may be given orally or in writing on a physical or digital copy, but it must be recorded.

A controller must notify the Information Commisioner's Office (ICO) within 72 hours of the discovery of a data breach, unless the controller can demonstrate that the breach is unlikely to result in a risk to data subjects.

Fines

Fines under the GDPR can have a significant impact on small organisations. For more severe breaches, fines of up to €20 million or 4% of annual turnover, whichever is higher, could be levied. For less severe breaches, fines of up to €10 million or 2% of annual turnover, whichever is higher, could be levied.

However, these extreme fines are not likely to be applied to small organisations and community nonprofits. Administrative fines are discretionary rather than mandatory and are to be imposed on a case by case basis in a manner that is “effective, proportionate, and dissuasive.” A reprimand may be issued in place of a fine in the case of a minor infringement or where a fine would impose a disproportionate burden on an organization.

Behaviour is taken into account when determining the severity of a fine, so organisations that actively report a breach and work quickly to remedy a fault will likely be given more leniency.