The Data Protection Handbook

A Guide to compliant management of personal data with reference to the GDPR.

Drafted by Sytorus Ltd.

For

The Irish Pony Club's members and volunteers

Contents

The purpose of this Handbook
The purpose of this handbook is to provide practical guidelines for organisations in order to manage their staff, volunteers' and supporters' personal data in a compliant manner.

The Irish Data Protection legislation sees the organisation itself (the legal entity) as the Data Controller, "the organisation which, alone or with others, determines the processing and use of the personal data". Staff and volunteers who gather and process personal data, therefore, are doing so on behalf of the organisation, and must comply with the organisation's data management procedures in order to protect its reputation and to avoid breaches of the legislation.

Compliance with this national legislation is enforced by the Office of the Data Protection Commission, based in Portarlington, Co. Laois, and will be based on the 7 Principles embedded in the General Data Protection Regulation (GDPR), an EU Regulation that will replaced the national DP standard in May 2018. Any data management policy used by the organisation must comply with the 7 principles of the GDPR from May 2018 onwards.

Compliance with the legislation can be seen from three perspectives:
Personal: The personal data which the organisation processes relates to the staff and members of the organisation and their families, as well as to visitors to the organisation's premises and those who provide services to the organisation;
Professional: Even within an amateur organisation which relies heavily on the work of volunteers, the legislation requires that data is managed in a compliant and appropriate manner;
Reputational: Any breach of the legislation reflects negatively on the credibility and reputation of the organisation, and damages peoples' trust. Managing personal data in a compliant manner reduces the risk of this happening.

Introduction
Most organisations depend on volunteers to manage its day-to-day activities, with some staff employed to run the organisation's offices and meet its administrative obligations.

The Irish Data Protection legislation makes no distinction between the status of the data management activities of the employees of a commercial or charitable organisation, and the processing activities of volunteers on behalf of a sports organisation, charity or membership association.

The only distinction is this – employees process data within the terms of their contract of employment; since volunteers have no such employment contract, the processing which they carry out must be closely managed by the organisation. While volunteers would not be required to sign a formal contract with the organisation, they should be made aware of their obligation to process data in a compliant manner, and they should comply with the organisation's general policies on confidentiality and data security.

In the unfortunate event of a breach of the legislation, the Data Controller (in this case, the organisation) is equally liable, whether the breach is caused by an employee or a volunteer.

In managing their day-to-day activities, an organisation must collect and use personal data about its members and visitors for a variety of purposes. These purposes include:

- the organisation and administration of individual organisation memberships, annual renewal of registration of members and officers, new member registrations, etc.
- the disclosure of this personal data to appropriate authorities, governing bodies, national organisations, members and officers

- the administration of the organisation's activities (weekly Executive Meetings, group meetings, team management, appointment of mentors, preparation for competitions, training of mentors, judges and leaders, award ceremonies, AGM's, etc.)
- compliance with statutory obligations (including Garda Vetting, Health and Safety, Child Protection procedures, etc.)
- Information on injuries, medical treatments, and the processing of insurance claims for members injured while participating in organisation activities
- Correspondence with members regarding organisation and group activities
- Bookings and administration of organisation facilities, such as function and meeting rooms, etc.
- Promotion of the organisation's social, promotional and cultural events
- Any fund-raising activities of the organisation

The Irish Data Protection legislation safeguards the privacy rights of individuals in relation to the processing of their personal data. When organisations gather personal data (data relating to living individuals) for any purpose, they must comply with the obligations of this legislation. In addition, as of May 2018, organisations will be obliged to comply with the GDPR, which will be automatically enforced throughout all EU Member States, and which will serve to increase the rights of the Data Subject, as well as increasing the responsibilities of the Data Controller.

There are two relevant pieces of legislation:

- The EC Electronic Communications Regulations (2011) and
- The Irish Data Protection Act (2018), arising from the General Data Protection Regulation

These Acts place responsibilities on those persons or organisations processing personal data, as well as conferring rights on individuals as to how their data is managed.

Definitions

The following terms are defined within the legislation:

"Personal Data"	means data which relate to a living individual who can be identified directly from that data (such as a name and address, or photograph), or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller or Data Processor (such as a membership number, PPS Number or car registration number). Personal Data also extends to data which is capable to directly or indirectly identify a person, such as online identifiers, location data, IP Addresses, etc.
"Special Categories of Personal Data"	processing of Personal Data involving racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
"Processing"	means performing any operation or set of operations on the personal data, whether by manual or automated means. This includes data collecting, organising, storing, altering, disclosing, sharing or adapting.
"Data Controller"	means any organisation responsible for the processing of the personal data.
"Data Processor"	means any organisation or individual which processes personal data on behalf of the Data Controller, but is not an employee of the Data Controller. This would include any third-party organisation using member data to help the organisation with direct marketing, fund-raising, member registrations, etc.
"Data Subject"	means a living individual who is the subject of the personal data.

Principles of Data Protection Legislation

Organisations must manage the personal data which they gather based on the following seven Data Protection Principles enshrined in the GDPR:

Principle 1- **Lawful, fair and transparent processing:** The Organisation must obtain and process personal information fairly, with the clear knowledge and awareness of its members. As much as possible, the organisation should explain what it plans to do with the data, and be able to justify the processing, if asked.

Principle 2- Purpose Limitation: The organisation must keep the data only for one or more specified and lawful purposes, such as the purposes outlined above. Organisation members and volunteers should avoid using the data for anything other than these purposes.

Principle 3- **Minimisation of Data Processing:** The organisation must only use and disclose the data for the purposes agreed by the organisation. Typically, this will include membership administration, payment of subscriptions, correspondence with members and notifications about events.

Principle 4- **Accuracy and Currency:** The organisation must keep the personal data as accurate, complete and up-to-date as possible. The organisation should have procedures that ensure high levels of data accuracy and to ensure that personal data on members, volunteers and service users are kept up-to-date.

Principle 5 – Limited Retention in a Format Which Permits Identification: The personal data should only be retained for as long as necessary in a format which permits the identification of the individual, in order to satisfy the specified purpose(s), or as required by law and should then be put beyond use or verifiably destroyed in an appropriate and secure manner.

Principle 6- Data Security and Integrity - Protection of Individuals' Privacy: At all times while the data is within its care, the Organisation should keep the data safe and secure from unlawful or unauthorised access, modification or deletion.

Principle 7- **Accountability and Liability:** The GDPR requires that the Organisation, and, in turn, associated service providers or Data Processors, should be able to demonstrate their 'culture of compliance' with reference to tangible evidence of an embedded series of processes, data management protocols and governance structures.

In the following section, we will look at different ways in which organisations can process personal data in their day-to-day activities, while remaining in compliance with the legislation.

Responsibility and Liability

While the organisation has ultimate responsibility for compliance, all members, staff and volunteers who collect and process the personal data on behalf of the organisation need to be aware of their responsibilities under the Data Protection legislation. The organisation should provide this Handbook as a guideline to all members and volunteers to ensure that they are aware of their obligations under the legislation.

In certain circumstances, the Executive Officers of a club or organisation can be held individually liable for breaches of the Data Protection legislation, where the breach is found to have been caused by their direct involvement, negligence or 'connivance'. Such liability is currently capped at €50,000 per person.

The organisation should also advise members, staff and volunteers of the appropriate procedures to follow in relation to data acquisition, storage, disclosure and processing.

Note:
The following scenarios are intended to provide examples of best practice regarding data management during the typical activities of any member or volunteer organisation. They are meant as general guidelines only - this is not legal advice.

If your administrative activities involve other processing of personal data on a regular basis, please seek direction from your own head office at Irish Pony Club, Main Street, Urlingford, Via Thurles, Co Kilkenny or jane@irishponyclub.ie or seek advice from the Office of the Data Protection Commission (www.dataprotection.ie), or contact Sytorus at https://www.PrivacyEngine.io for further information.

Scenario: Communication with Members

Responsibility

Members of the Executive and Organisation officers should be responsible for the management of any communication which is sent out on official organisation note-paper, or claiming to be on behalf of the organisation. This does not mean that only one person should send every communication. However, anyone sending communication or correspondence on behalf of the organisation, or using the organisation members' contact details to do so, should be made aware that the communication must be in compliance with the GDPR, as outlined in its seven Principles (above).

The EC Electronic Communications Regulations (2011) introduced specific obligations for any organisation using electronic media (calls to landline, fax or mobile phone, as well as SMS, e-mail or social media messaging, e.g., Facebook) to send marketing or promotional messages.

Servicing v Marketing Messages

The club or society can differentiate between communications which are integral to the enjoyment of membership of the organisation, and which are expected by the members due to the nature of the organisation's activities, such as reminders about events and registration, notification of a change of time for training, or a change of venue for a competition, etc. (servicing communications) and communications which the organisation wishes to send in order to promote or advertise products or tickets to an event (marketing communications).

As long as the club or society sets reasonable expectations at registration, servicing communications are permissible without prior consent. However, under the 2011 Electronic Communications Regulations and the GDPR, the organisation must have ***prior, clear, freely-given consent*** from its members and non-members before sending out electronic marketing communications.

Things to Do:

- For postal communication, the organisation should have headed note-paper, and only authorised members of the Executive should have access to such material, in order to control the number of people representing or speaking on behalf of the organisation.
- Anyone sending communications on behalf of the organisation should ensure that this is carried out with the approval of the organisation's Executive Panel, e.g. the organisation Secretary or a senior Officer.
- Anyone sending electronic marketing or promotional communications on behalf of the organisation, whether by e-mail, SMS or via social media, should ensure that they have the prior consent of the recipient to contact them in this manner. Consent here must be "freely given, specific, informed and unambiguous, involving an active indication of the individual's preference." The data subject's consent must be clear (Principle 1 – Fair and transparent processing).
- Any communication from the organisation should include contact details for the sender or an organisation officer, in case the recipient needs to seek clarification or follow up on the content of the communication.
- The club or society should confirm the appropriate contact details for each member at registration – this includes the details of the parent(s) or guardian(s) to be contacted in relation to each underage or child member (those under 18 years of age).
- Where messages are being sent via social media, WhatsApp or other group text facilities, it is important to ensure that the purpose and content of the message is confined to the purpose for which the group was set up – for example, if the WhatsApp group was set up to inform parents about upcoming events, times of training or deadlines for registration, then the content of any message sent via this Group must be limited to those purposes. (Principle 2 – Specified and Lawful Purpose).

- E-mails sent by organisation officials to several recipients at once should always use the bcc ("blind copy") field to prevent the unnecessary disclosure of recipients' e-mail addresses to others (Principle 3 – Minimisation of processing).
- Messages relating to the activities of children and under-age members (those under the age of 18) should be sent directly to their parents or guardians, not to the minors themselves.

Things to Avoid:

- The organisation should not correspond directly with any organisation member under 18 years of age. Any correspondence to juvenile members must be through their parents or guardians, using details provided at registration. The organisation should take reasonable steps towards confirming the authenticity of the parental consent, where appropriate.
- The organisation should not contact individuals for marketing or promotional purposes who have already asked not to be contacted for these purposes.
- Since consent should involve an active indication of one's preference, the organisation should avoid using 'pre-ticked' boxes on any registration or application forms.
- The club/society should avoid making assumptions as to the consent or preferences of its data subjects/members. Consent must be unambiguous, in order to be considered adequate under EU Law.

Scenario: Registration of members

For most organisations, annual registration is one of the most important times during the calendar year when the organisation interacts directly with its members. It is also the most important data processing opportunity for the organisation, and it is vital to get it right. This section also applies to registration forms for organisation activities, 'away days' and trips, as well as application forms for competitions.

Responsibility:
Should the organisation have one or more Executive committees, e.g. local, regional and national, etc., the Registrar/s should have overall responsibility for the management and processing of registration. Team leaders, coaches and managers may collect the data directly from current and new members, etc., or instruct new members to register online (where that facility exists).

The organisation Executive should ensure that membership and application forms are designed to get the full range of data required from members for the administrative purposes of the organisation but are limited to seeking only the minimum amount of data necessary to satisfy these requirements.

Forms may vary depending on whether the organisation differentiates between adult and junior members, but ideally, the organisation should use one registration form which will satisfy all requirements.

Things to do:

- Ensure that the membership registration forms and competition entry forms include fields for all data items which the organisation requires, in order to meet its purposes - including contact details, date of birth, parent/guardian details for junior members, dietary requirements, medical conditions, allergies, etc.
- Include contact details of the organisation's Data Protection Officer, where applicable, so that registrants or applicants can contact the organisation to seek clarification on any point.
- Ideally, organisations should have a nominated person responsible for the gathering and management of applicant data, who will be available to members (and their parents or guardians) to answer any questions they might have regarding the processing of such data.
- The club or society should familiarise themselves with the guidance around the designation of a Data Protection Officer (Article 37 GDPR).
- At membership registration, all members must be informed about the purpose or purposes for which their personal data will be used. In addition to the administration of their membership, this might include processing of subscriptions or bank payments and the sending of 'servicing' messages (e.g. notifications about organisation events, leadership training, fund-raising events and other organisational activities).
- If space permits, the form should provide a brief narrative for each field on the registration form, explaining why the data is needed and setting reasonable expectations with those providing their personal data regarding how that data will be used.
- Separately from registration for membership of the organisation, the registration form must offer members a separate, clear option to 'opt in' for the organisation's promotional and fund-raising activities. Where members do not give their consent, the organisation should make sure that they are not contacted for this purpose. Members must be offered an option of selecting an "active opt in" in order for this consent to be valid.
- Prospective members should be informed in advance of their right to withdraw consent from receiving promotional messages at any time. Under the GDPR, individuals have generally stronger rights to withdraw consent in regard to the processing of their personal data and organisations should reflect this in their registration forms.
- The organisation should ensure that all membership forms are collated and brought to a central storage point as soon as possible, once the forms have been completed and submitted.

- Where possible, the organisation should minimise the amount of paper forms being used – where members register using paper forms, the organisation should try to transfer this information to computer as soon as possible, as data in this format is more secure and more efficient to store and retrieve.
- Where it has been possible to type the details from paper registration forms into the organisation's computer system, the original paper forms should either be filed and stored securely in a central location, or should ideally be shredded and destroyed. Organisations should implement their own policy to this effect, encouraging good practice in the long term.

Things to Avoid:

- The form must not ask for members to provide data which the organisation does not intend to use – if there is no current processing requirement for it, the organisation should not seek the data on the registration form.
- The form should not label individual fields on the form as 'mandatory' unless there is a formal, legal requirement for that item of data. Where such a formal requirement exists, the organisation should explain the legal obligation associated with the item of data.
- The organisation should not assume that members will want to be contacted for marketing or promotional purposes, just because they are staff, members or supporters of the organisation. The form must offer individuals an option to actively opt in, NOT an option to opt out.
- Application forms submitted at local club branches or offices should be sent through to the organisation's central office as soon as possible, and should be stored centrally and securely.

Scenario: Managing Data Security

Failure to keep personal data safe and secure is one of the biggest causes of breaches of the Data Protection legislation, and one of the most damaging things that can happen to an organisation, since it undermines the members' trust in their organisation, as well as damaging the organisation's reputation and the credibility of its Executive and of its 'brand'.

Responsibility

A member of the organisation executive, usually the Registrar, should be accountable for the data held by the organisation, controlling who has access to it, where it is stored, and how it is transported or transferred elsewhere.

The responsibility for the security and safety of the personal data which is held by the organisation rests with each member who has access to that data. Whether in paper or electronic form, the data is a valuable asset, and should be treated with the same respect as the organisation's premises and its fixtures and fittings.

Appropriate security solutions will vary depending on the volume, value and format of the data held by the organisation, and may include measures like encryption of laptops, mobile phones and storage devices (USB sticks, external hard drives, etc.), password protection on all files containing sensitive personal data, and locked cabinets at the organisation's offices in which all paper records are stored when not in use.

The obligation regarding data security also extends to the physical security of the organisation's premises, the number of key-holders who have access to the premises and individual offices, deployment of CCTV cameras on the organisation's grounds, etc.

Things to Do

- The organisation should have a Data Security policy which outlines the rules regarding acceptable use of the organisation's data, how it should be stored and transported, and who should have access to it.
- Any organisation member who has access to the data should receive training regarding their responsibilities, should be familiar with this Security Policy and should adopt the appropriate security measures when processing the data.
- Whenever possible, the organisation should minimise the amount of personal data which is stored or processed away from the organisation's premises.
- It is inevitable that organisation officers and leaders will hold their own records on organisation members (group lists, parent contact details, etc.), but such records should be kept to a minimum, and should be stored securely by the organisation's members while in transit or in use. This particularly includes circumstances where club members or officers take data from the files or office in order to attend meetings and conferences, conduct training or coaching events, etc.
- Where possible, the organisation should take a regular back-up of its electronic data records, so that in the event of a catastrophic incident (fire or flood damage to offices, etc.), normal organisational activities can be restored in a timely manner.
- Organisation officials should challenge the 'need to know' of any organisation members regarding the level of access which they have to members' data – access to data should be based on a person's specific role within the organisation, rather than simply because of their membership or seniority.
- Where the organisation engages the data management services of any third-party organisation, a formal Data Processor Agreement must be in place before any of the organisation's data is disclosed to the third party (a contract template is available from Sytorus, if required).
- The organisation's computer equipment should be password protected, and access codes should not be shared between officers, or left somewhere that is easily accessed.

- The organisation should adopt a 'clean desk' policy at its premises. Paper files should be locked away at the end of each working day, and when not in use.
- Data in both electronic and paper format should be transported and stored securely when being used away from the organisation's premises and should be deleted or shredded once they are no longer required.
- The organisation's premises and individual offices should be kept securely locked when not in use.
- Doors, filing cabinets and desk pedestals in the organisation's offices should be locked at the end of each working day, or when the offices are unoccupied.
- Staff and volunteers should 'lock' their computer screens (by pressing CTRL + ALT + DEL) when they leave their desks unattended, even for a short time.
- The organisation should introduce a 'Leaver/Mover' policy to keep track of staff members and volunteers, and the level of access they have to systems and data files. Where someone leaves the organisation, or moves to a new role, this should be logged, and their access to the systems should be withdrawn or changed appropriately, as soon as possible after their move or departure.
- Appropriate training, in the form of instruction at induction stage, regular refresher training, and this Guidance Handbook, should be made available to all staff and volunteers.
- Where CCTV has been deployed at the organisation's premises, the organisation should appoint a senior member to be responsible for its maintenance and management. The Office of the DP Commission provides separate, specific guidelines regarding the management and use of CCTV within an organisation, and the organisation should ensure that they are familiar with these guidelines.

Things to Avoid

- Data should not be stored on unencrypted or unsecured devices – Executive members, Managers, Leaders volunteers and staff who hold copies of personal data on their personal computers or mobile device should ensure that those devices are secure.
- If possible, any electronic correspondence involving the personal data of staff, volunteers and members should be conducted over secure, encrypted networks, rather than over publicly-available and non-secure networks such as G-mail or Hotmail.
- Where personal records are saved on a mobile device or laptop, they should be saved in a secure, password-protected folder, and never on the C: -drive or desktop of the device.
- Paper records should not be taken from the organisation's offices unless it is absolutely necessary. Copies of personal data, used for a particular purpose or event, should be returned to the organisation's secured files and any unnecessary copies should be destroyed as soon as that purpose or event is completed.

Scenario: Breach Management and Notification

Responsibility:

Under the GDPR, any incident which exposes staff or member data to risk must be notified to the Office of the Data Protection Commission within 72 hours of the organisation becoming aware of the breach. The Commission has provided a form on its website (www.dataprotection.ie) which must be completed by the Data Protection Officer (DPO) or a nominated offer of the club or society, and which should include details around the incident, the circumstances leading up to it, its consequences, and what has been done to minimise the impact, as well as to prevent a recurrence.

Things to do:

- Once the organisation becomes aware of an incident or breach, the DPO or a senior club member should be placed in charge of managing the incident
- All those involved in, or aware of the breach should be asked for their input regarding the incident, how it occurred, and the extent and impact of the breach (whether it involves the loss, destruction, disclosure or mismanagement of personal data).
- The nominated incident manager should prepare a response to the incident, using the questions contained in the template provided by the DP Commission as a guide.
- Where the incident poses a risk to the data subjects whose personal data has been compromised (e.g. the loss of their credit card numbers or bank details, the disclosure of sensitive or confidential information, etc.) the organisation should send out a notification, either individually or through social or public media, to make them aware of this incident, and the possible consequences, as soon as possible.
- Where a third-party organisation was involved in any aspect of the incident (e.g. an IT service provider or partner organisation), their input to the circumstances as well as the resolution of the incident should be sought as quickly and constructively as possible.
- The organisation should submit a report of the incident to the Office of the DP Commission as soon as possible once the details are known, but in any event, within 72 hours of first being made aware of the incident.
- The organisation should make every effort to retrieve or recover the data which has been compromised, as well as to put measures in place to prevent a recurrence. Where a system or process has been found to be insecure or faulty, the organisation should suspend their use of that system or process with immediate effect, until the cause of the problem can be identified and fixed.
- Once the cause of the incident is known, office staff and senior club members should be informed and provided with appropriate training to ensure that the risk of a recurrence is minimised.
- Where the incident is found to have been caused by unlawful or non-compliant actions of a third party, the organisation should invoke the appropriate clauses in the Data Processor Agreement to penalise the third party for any damage caused to the activities or reputation of the organisation.
- Where the incident is found to have been caused by the mis-management of personal data by a member of staff or volunteer within the organisation, the club should pursue appropriate disciplinary measures to penalise the individual involved, and to raise staff and volunteer awareness in order to prevent a recurrence.
- Any communication by the organisation in relation to the incident should be controlled and managed through the DPO or a senior officer, to minimise misinformation and minimise the risk of worry or distress on the part of club staff or members.
- The organisation should initiate some form of training to raise awareness around the process for breach detection, evaluation and formal notification.

Things to Avoid:

- Where the breach or incident poses risk to the welfare or confidentiality of individual members, staff or volunteers, the organisation should not consider suppressing or withholding information on a Breach from the Office of the DP Commission – to do so would be an offence under the GDPR. If the Commission were to become aware, at some point in the future, that the organisation withheld or failed to report the incident, the club or society could be prosecuted under Article 83 of the GDPR, with severe financial and reputational consequences.
- Where the club or society has confidence that the incident will not pose a risk to individual members or staff, there is no obligation to report to the Office of the DP Commission (e.g. where a laptop or USB stick is lost or stolen, but the device has been encrypted, there is no risk that the data contained on the device will be accessed, therefore no risk to the individual data subjects).
- There should be no interim or unauthorised disclosure of information in relation to the incident – club members should refer any questions or concerns to the DPO or the senior Executive member who has been nominated to manage the incident.
- The organisation should avoid any unnecessary delay in the notification process, both in respect of the supervisory authority and also the individual data subject, where appropriate. Time is of the essence, both in terms of recognition of a breach and notification to the relevant body or individual(s).
- Staff should be trained so that they are familiar with the detection and recognition of DP breaches that may occur inside the organisation, as well as being able to recognise the severity of the risk to the confidentiality and privacy of data subjects/ individual members.

Scenario: Requests for Disclosure of Personal Data

Responsibility:

From time to time, organisations may be asked to provide or disclose information about its staff, volunteers or members. In such circumstances, the organisation needs to exercise its responsibilities as a Controller of that data, and set strong challenges to any such request for disclosure, until its officers can determine that the request for disclosure is legitimate, appropriate and lawful.

Things to do:

- The club's or society's officials should challenge the basis for any request for disclosure of personal data held by the organisation. Even where a request is legitimate and justified, the organisation should only release the minimum amount of data necessary to satisfy the request.
- The organisation must be satisfied that the individual or organisation making the disclosure request is authorised to do so – whether they are a parent or guardian of a juvenile member, a member of An Garda Síochána, or an officer of the respective National Governing Body for the sport or activities of the organisation.
- Registration forms should seek clear information on the identity of individuals who are authorised to seek information on juvenile members – this is particularly important where the parents of a young member may be living apart, but are equally involved in supporting the child's membership and activities at the club or society.

Things to avoid:

- The personal data of organisation members should not be generally available, and only the minimum amount of data should be provided to those who need it.
- The organisation should never disclose members' personal data, either individually or in volume, to another organisation without legitimate reason. If requested, the organisation should act as the 'gate-keeper' for the data, and should remain in control of any use of the data or any access to it.
- No personal data should be disclosed by the organisation unless a formal request in writing has been received, and unless the organisation has been able to verify the identity of the requestor, and their authority to request such information.

Scenario: Records Retention and Destruction

Responsibility:

Organisations will need to keep certain categories of personal data for different periods of time – in some cases, in order to provide administrative services, in other cases to meet its legal obligations or maintain a historical archive of the organisation. The organisation needs to strike a balance between satisfying its legal and archival obligations, and minimising the risk of data loss by removing or destroying any data which is no longer required for operational purposes.

The difficulty for many organisations is in deciding what to keep and what to destroy. With electronic records, today's technology allows organisations to keep data for longer, at very low cost. Paper records can eventually take up a lot of space, and become a nuisance for the organisation if they are not properly managed and efficiently or securely stored.

The key principle of the GDPR is that the organisation is encouraged to keep the data only for as long as necessary in order to achieve its operational and legal objectives (e.g., administration of membership, processing of payroll and employment obligations, reporting to Revenue and National Governing Bodies, retaining information for insurance or legal purposes, etc.).
Therefore, it is not a question of the organisation's network or system capacity or the available storage space, but how soon the data records can be destroyed or removed.

Things to Do:

- The organisation should be aware of its legal obligations in terms of retaining administrative and financial records – for reference, check the guidance on the website of the Office of the DP Commission, at http://www.dataprotection.ie.
- The organisation should draft a Data Retention and Destruction Policy based on these obligations
- The organisation's Executive, managers, leaders, volunteers and staff who have access to personal records should be aware of the Retention and Destruction Policies, and they should ensure that records are only kept for as long as necessary with reference to these Policies
- The organisation needs to remember that the retention obligations apply equally to electronic and paper-based records
- As much as possible, personal records of organisation members and staff should be collated and returned to the organisation's premises for longer-term storage and retention.
- Once it has fulfilled its operational objectives and is no longer required by the organisation, any correspondence which contains personal contact details, whether old letters and invoices, application forms, post-it notes or addressed envelopes, should be shredded before being disposed of in the rubbish.
- The organisation's master records should be held at the organisation's premises, and in secure storage, rather than spread among a number of the Organisation's officers and volunteers, or held at their homes or places of work.
- Computer equipment used by the organisation to process personal data should be wiped or de-gaussed with an industrial magnet to remove any trace of the data prior to the device being sold or recycled.

Things to Avoid:

- The organisation should not keep records for longer than agreed in the Retention Schedule.
- The organisation's Executive, Managers and leaders should not keep copies of the organisation's personal data records at their homes when the original records have been destroyed as part of the Retention and Destruction Policy.
- Personal data in paper form should not be simply thrown in the rubbish – records should be shredded before being disposed-of.
- Computer equipment on which the organisation's data had been processed should not simply be sold on or recycled without first being professionally 'wiped' to delete any personal data from the hard drive.

Scenario: Fund-raising and Promotional Activities

Organisations are constantly seeking new and creative ways to raise funds and ensure continued financial support for the organisation. While organisations raise revenue from events and functions, the most effective method of fund-raising is to run a direct marketing campaign among the organisation's membership and members of the public. While members will often be supportive of the organisation's fund-raising efforts, the organisation cannot make assumptions about their consent to be contacted for such purposes.

Since the EC Electronic Communications Regulations (2011), any marketing or promotional activity using electronic media must meet an additional set of obligations, including the prior, clear consent of the individual to be contacted for such purposes.

Responsibility:
The organisation should appoint an Officer with responsibility for fund-raising, who will decide what campaigns are run, how frequently and what data, or categories of data, to use.

Things to Do:

- Members should be informed at registration that their personal data may be used for marketing and fund-raising purposes. They should be given the option to 'opt in' for such use of their data
- At registration, the option to opt in to receive marketing messages should be separate and quite distinct from the registration process. An individual can register to become a member of the organisation without opting in to receive marketing material, and vice versa.
- In any subsequent fund-raising literature, recipients should be given the option to 'opt out', and to stop receiving such messages.
- On receipt of an 'opt out' notification, the organisation should block their record as soon as possible, but in any event, within one month of receiving their 'opt out' notification.
- Where an organisation engages a third-party specialist to run their fund-raising campaign, a formal contract must be in place before any personal data is processed by the third party (the Data Processor Agreement).
- Where members have given consent to be contacted for marketing and fund-raising purposes, their data must be used for that purpose at least once in each twelve-month period from the date their consent is received.
- Newsletters which are sent to the organisation's members about the organisation's events, training and operations can be used for fund-raising purposes, and are therefore considered marketing material. Members should be asked to provide a clear indication of their consent to receive such newsletters.
- Prior to sending out a marketing campaign message, the organisation should cross-check the distribution list against the list of those who have previously 'opted out', to ensure that no-one is contacted without their consent or against their preference

Things to Avoid:

- Just because the organisation has the contact details for members, this does not mean that their data can be used for marketing purposes. Their clear consent should be sought for this secondary purpose.
- Fund-raising messages should not be sent directly to organisation members under 18 years of age without prior parental or guardian consent.

Scenario: Involvement of Third Party Service Providers

From time to time, the club or society may need to see the services of a third-party specialist to assist them in their work – for example, a recruitment company to find new staff, an accounting firm to help with payment of payroll, or an IT service provider to install and maintain the organisation's network infrastructure.
Where these third parties will have access to the personal data held by the organisation, (whether or not this is directly intended) they are known as Data Processors, and the club or society must ensure that a formal contract, known as the Data Processor Contract, is in place before the third party has access to any of its personal data.

Responsibility:
While the third-party service provider may produce their own contract template for this purpose, the obligation to ensure that such a contract is in place rests with the Data Controller – in this context, the club or society.

Things to Do:

- The club or society must ensure that the service provider being sought to deliver the service is competent, reliable and understands its obligations under the DP Regulation.
- The organisation must ensure that the formal, written contract is in place prior to the third party having any access to the personal data for which the organisation is responsible.
- The clauses of this contract must include reference to the twelve topics mandated for inclusion by the GDPR – including an obligation to confidentiality when processing the data, the security of the information in question, an obligation to process the data within conditions or parameters set by the Data Controller, etc.
- The terms of the contract should be reviewed on a frequent basis, no later than annually, and the Controller must ensure that the Data Processor complies with all terms of the contract at all times while the data is being processed.
- Where the Data Processor engages the services of other organisations to further assist with the processing of the personal data (a sub-contractor), the Processor must notify the club or society in writing about this appointment, and the club must have the option to veto or challenge any such appointment.

Things to Avoid:

- Third parties must not be allowed unaccompanied access to the network, files or office premises of the Data Controller (the club or society) without this contract being in place – regardless of how short the engagement of the third party may be.
- At the end of the contractual engagement, the third party must not be allowed to keep the data disclosed to them during the course of the contract. The third party must either return such data, or provide the club or society with a written undertaking that any such data has been verifiably put beyond use or destroyed, unless there is a legal obligation to retain it for any purpose.
- The organisation should not simply engage a third party on a referral or recommendation – some effort must be made by the organisation to verify and evaluate the third-party provider's competence and compliance prior to engagement.

Scenario: Data Processing Activity Logs

Under the GDPR, Data Controllers are required to input and maintain Data Processing Activity Logs for each type of personal data processing they encounter. It is good practice for the organisation to outline the lawful purpose for which the personal data is being collected, as well as describing each processing activity with reference to the headers included in Article 30 of the GDPR.

Formally, under the GDPR, this obligation only applies to organisations with more than 250 employees. However, many clubs and societies meet this threshold if the data processing activities of both staff and volunteers are taken into account. Even where this is not a mandatory exercise, organisations find that this is a valuable thing to do, as it helps clubs and societies to focus on the range, diversity and depth of data processing which takes place within the organisation.

Responsibility:
Organisations with more than 250 employees (including volunteers) are required to input and maintain Data Processing Activity Logs

Things to Do:

- Promote good compliance practice by logging and describing each data processing activity in a secure data processing activity log or spreadsheet.
- Maintain this log diligently in order to have a full record of each category of personal data that the organisation processes, as well as the details on who processes the data (e.g. staff, volunteers, third party service providers, etc.).
- Include a detailed summary of the reasoning for the data processing activity, along with the lawful processing activity attached to this. E.g. consent of the individual, a contractual or legal obligation, or the legitimate interests of the club or society.
- Staff and volunteers should review the processing log so that they are aware of what is being done, by whom the data is being processed, and the lawful purpose for each processing activity.

Things to Avoid:

- Once the organisation determines to conduct this exercise, all processing activities involving personal data should be included.
- Where processing activities are indicated as being completed by a third-party service provider, the organisation should take care to ensure that the appropriate contract is in place with each service provider.
- Once complete, the processing activity log should be saved and stored for reference, as well as to provide as evidence to the DP Commission if requested.
- As the organisation adopts new processing activities, or introduces changes to the way data is being processed within the organisation, it is critical that the logs are updated to reflect any such changes (e.g. where an in-house function is outsourced to a third-party service provider, etc.).

Scenario: Use of photos and video images

Photographs and video images capture the personal data of individuals, and must therefore be managed in compliance with the DP legislation.

Responsibility:

As the organisation on whose behalf the images or footage is captured, the club or society is the Data Controller, and must therefore ensure that any processing of the images is done in an appropriate and compliant manner.

Things to Do:

- Where the organisation plans to capture photographs of an upcoming event or competition, those attending should be notified in advance, where possible. This might mean that the club places a notice on the poster or tickets to the event, such as 'Please be aware that photos taken at the event may be used by the club in the future for promotional and publicity purposes'.
- At the event itself, we recommend that discrete but visible posters remind attendees that photographs will be taken.
- Where CCTV is in operation at the club's premises, clearly visible notices (the 'Fair Processing Notice') should be displayed, making members and visitors aware that their video image is being captured, the purpose for doing so, and the contact details of the DPO or a senior officer of the club, should they have any questions or concerns.
- The CCTV system should be regularly serviced and maintained, so that the images captured can be used for the purpose for which the system was installed – namely, the prevent or investigation of unlawful or unauthorised activity, access to the club's premises, or misuse of the club's facilities.
- Where photos are taken at the event, the photographer should make it clear to those captured in the image that the club would like to use the image, with their consent. Where their consent is forthcoming, the photographer should not the fact. Naturally, where anyone captured in the images objects, this photo should not be used by the club for any purpose.
- Where photographs taken at an event contain images of children or minors, the club or society must seek the clear consent of that child's parents or guardians before using the image for any purpose in relation to the organisation.
- While it is not mandatory to get such consent in writing, we recommend that the photographer seek to get clear, unambiguous permission from the individual at the time the image is captured, in order to avoid or prevent any dispute with regard to the use of the image in the future.
- Where the club or society engages the services of a professional photographer to capture images during an event or competition, the organisation must put a Data Processor Agreement (see above) in place with the photographer beforehand, setting clear expectations regarding the capture, use, storage and retention of such images.
- Photographs and images should be stored and indexed with reference to the event at which they were captured, and the individuals depicted in the images, in order to be able to retrieve the images at some point in the future if they are requested for disclosure or publication.

Things to Avoid:

- Photos and images taken at club or society events should not be published without the clear permission of the individuals captured in those images. Where it is not possible to get permission from everyone in the image (for example, a large crowd or grouping), the club should make every effort to make them aware, beforehand, that the image will be published on the club's web-site or posted on social media, and remind them that they have the option to object to such use of their image at any time.
- Photos and images should only be held for as long as they useful and relevant to the work and activities of the organisation, and should then be either archived or destroyed.
- Photos and images (including CCTV) should only be used for the purpose for which they were captured, and staff or volunteers should not have open or unlimited access to such images, in order to prevent or minimise the risk of their unauthorised or excessive use.

Scenario: Right of Access by the Data Subject

In compliance with the GDPR, any individual whose personal data is held by the organisation has the right to receive a copy of the personal data that is being kept about them by the organisation, either on computer or held in manual (paper) format in a filing system.

Any person who wishes to invoke this right can submit a valid Subject Access Request (SAR). There is no formal template for such a request. A request is valid once it meets the following two criteria:

- The request must be writing
- The requestor must provide adequate proof of their identity

The organisation will then have a maximum period of one month to respond to a valid request. The organisation should try to respond to the request in the shortest possible time.

The organisation cannot charge a fee for responding to this request. However, a reasonable fee can be charged subsequently, where the individual requests a copy of the material already provided.

A copy of the resulting data should be provided to the requestor in printed format, with the organisation also keeping a full copy of the data provided, in case there is any subsequent dispute over the contents or scope of the data provided. Original documents should never be disclosed as part of a response to a Subject Access Request.

Where disclosure of personal data from the club or society is requested by another organisation, the club should determine whether the request is valid, whether the requestor is authorised to have access to the information, etc., and should seek a copy of the data request in writing. Even where it is established that the request is valid, the organisation should limit the range and scope of data being disclosed to the minimum necessary.

Where a member of staff requests contact details for another staff member or volunteer, we recommend that it is preferable for the organisation to liaise by taking a message and passing it on to the person in question, rather than disclosing one person's contact details to another.

Responding to Data Subject Rights

While this Handbook focuses on the Data Controller's obligations, we should remember that we are all Data Subjects, by virtue of the fact that the organisation is processing our data as members, volunteers, officers, etc.

The Data Protection legislation provides specific rights for Data Subjects, in addition to the set of Principles mentioned above. The following Rights are available to anyone whose personal data is being processed by the organisation:

- The right to access a copy of their data held by the organisation, as outlined above
- The right to have incorrect data, which relates to them, either corrected or removed
- The right to 'opt out' from receiving direct marketing material
- The right to prevent processing of their personal data which would be likely to cause damage or distress
- The right to have processing explained where decisions are made solely by automated processing
- The right to support from the Office of the Data Protection Commission
- The right to seek compensation in the civil courts, in the event that we feel our personal data has been misused
- The right to be Forgotten/ Erasure – the right to have their data removed from use, unless the club or society has a lawful reason for retaining it
- Right to Data Portability – the right to request that an individual's personal data be 'ported' or moved from one organisation to another – e.g. a club, bank, school or utility.

Under the GDPR, when any of these Rights are invoked by an individual, the organisation must be able to respond in a timely and appropriate manner, within no more than one month of receipt of the written request. The organisation cannot charge a fee for its response to these Rights.

Compliance with other Standards and Regulations

In addition to the GDPR / Irish Data Protection Act, all clubs, membership associations and sporting organisations must comply with obligations under a wide range of other legislation and standards, including employment and tax law, anti-money laundering, credit card security (PCI DSS), health and safety, child safeguarding, etc. In some cases, compliance with one obligation may appear to contradict or compromise compliance with another.

For example, in responding to a request from the Gardai regarding details about an organisation's member, that person's privacy rights may have to be set aside due to the over-riding concerns of the Gardai with regard to their investigations.
Where such a conflict arises, the organisation should feel free to seek legal advice, or to seek advice from the Office of the Data Protection Commission, before disclosing the data.

Further Information and References

Further, detailed information on Data Protection is available from a number of sources:

The office of the Irish Data Protection Commission at www.dataprotection.ie

The Office of the DP Commission has provided specific Guidance for the Irish Charity and Voluntary Sector at http://www.dataprotection.ie/docimages/CharityMarch14%201.pdf

Sytorus is an independent Data Protection consultancy and training organisation, based in Dublin. We can be reached through our web-site at www.Sytorus.com, or via our online, interactive knowledge base at https://www.PrivacyEngine.io