The GDPR in Brief
Under the GDPR, organisations to whom data subjects give their personal information to are more accountable to them. The accountability principle means clubs should comply with the GDPR and be able to demonstrate compliance.

Records of Processing Activities
If it is written down then it hasn't been done! Keeping written records is useful to demonstrate compliance under the GDPR. The definition given to the term is in Article 30 of the GDPR. This is where the data inventory is the tool of choice.

Fines
Fines may be imposed by supervisory authorities on a controller or processor.

Reputation
Special Olympics Ireland, as a registered charity, depends on the goodwill of the public for donations. Any failure of club volunteers to comply with legislation inevitably results in damage to the organisation's reputation.

Summary
If there is a breach of personal information the Data Protection Commissioner will need to be notified, as will each individual affected by the breach. This can cause major reputational damage as well as a large financial penalty.

Being aware of the risks to personal information and ensuring controls and mitigations are in place allows us to deliver on our personal information pledge.

What 7 actions can clubs take to keep on top of the GDPR?
1. Keep records accurate and up-to-date
2. Don't hold any information for any longer than needed for a particular purpose
3. Share a minimum amount of information purely on a need-to-know basis
4. Protect the identity of Email recipients by using Bcc (blind carbon copy)
5. Don't share passwords /password protect spreadsheets of names
6. Paper files – Store & destroy records safely.
7. Electronic files - Lock your computer/laptop screen when away from it.

Official Special Olympics Ireland Communications
Clubs should direct all press, television and other media enquiries to Special Olympics Ireland's Marketing and Communications Manager.

Subject Access Requests
- Free of charge under the GDPR (when effective) for the first copy of information.
- Relates only to an individual's own information and not third party requests. Take care where a third party asks you for personal information - prior consent of individual; respect wishes.
- Request must be in writing, it doesn't need to be on the official Special Olympics Ireland Subject Access Request Form. The more specific the data subject's request, the greater likelihood you can provide what they need promptly.
- Response must be provided within 30 days. Clubs may need additional time and may extend it by two months. The extension must be for a good reason and do the requester know this as soon as possible. Look at how you would respond to a request.

- Clubs may ask questions if you need to verify the identity of the requester and their relationship to an athlete. Clubs are entitled to ask for a relevant form of identifications.
- Clubs will need to be able to let subjects have information about the data they hold, that's where the data inventory is useful.

Subject Access Request Log
The Club Membership officer should maintain a log of Subject Access Requests.

Reasons a data security breach can happen
- loss or theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as a fire or flood;
- hacking attack;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

Security Breach Response Plan
Clubs will need to have in place a security breach response plan. This can take many forms, but the most practical is a three step process.

Recording: near misses and data breaches should be recorded in the club's data breach log; an outline of the breach; details of person reporting incident, date(s) of breach, date incident was discovered, if incident was reported to the other affected data subjects/ the data protection commissioner and recommended measures to mitigate any possible adverse effects from the breach.

Reporting: minor data breaches are not required to be notified to Special Olympics Ireland. Where a deviation is reoccurring and may result in identification of a serious breach, this should be notified to Special Olympics Ireland.
Major data breaches must be notified to Special Olympics Ireland within 3 calendar days of becoming aware of that data breach.

Escalation: Corrective and preventative actions should be implemented for any data breaches. It is recommended that reoccurring data breaches be discussed at any regional meetings and if required detailed in the Board Report.
If the data breach must be reported to the Data Protection Commissioner, please refer to their Code of Practice. The regulatory timeline under the GDPR is seventy two (72) hours of becoming aware of the data breach. A serious data breach may prompt Special Olympics Ireland to undertake a triggered audit of the club. All data breaches must be resolved to conclusion.

Privacy by design
This refers to data storage and security of access. In general paper files should stay under lock and key in a filing cabinet in a specified location, or at least be returned there immediately after use. If travelling on the road, keep files out of sight and locked in the car boot. Electronic files, such as spreadsheets containing sensitive information, require password protection and encryption. Encrypt computers/laptops - protects it if it is stolen. Encrypt or at least password protect USB sticks.
Special Olympics Ireland will password protect and encrypt the full list of registered athletes and volunteers that are sent to our clubs on an annual basis. Clubs must play their part by not sharing

their password. Due care should be taken at all times to ensure that data on any club member is held in a safe and secure location and all data is appropriately protected.

Data minimisation and privacy by default

This refers to ensuring, by default, that a minimum of personal information is being processed and it is shared only on a "need to know" basis. The club coach and officers on a Club Management have access to the information.

Special Olympics Ireland is reviewing the health data fields on the APF as part of the Athlete Participation Form (data minimisation) project.

Consent and lawfulness of processing

Where consent is the basis for processing it must be freely given and in the form of an "opt-in" action. Consent may be removed as easily as it was given. Where consent is the basis for processing, clubs should seek to also find alternative and/ or supplementary grounds for processing. Consent must be granular or broken-down into clear elements that may separately be selected.

Contact details for the Data and Records Manager

Address: Special Olympics Ireland Central Office, National Sports Campus, Snugborough Road, Dublin 15, D15 PC63, Ireland
Email: data@specialolympics.ie
Telephone: +353 1 869 1614 (direct)
+353 1 882 3972 (reception)
Website: www.specialolympics.ie