Data Protection Compliance

1. Increase Awareness

The GDPR benefits everyone by ensuring that our personal information is protected from misuse by any organisation. It holds each Squash Club, County, or Provincial Board accountable for how they collect, use, and store information about squash members. It is essential that every member understands the changes brought by the GDPR and how these changes impact them, either as a volunteer working on behalf of the club or as an individual club member.

This awareness also extends to our personal lives, as the GDPR affects banks, insurance companies, utility providers, online marketing, etc.

Clubs should ensure that information relating to the GDPR is made available to committee members, club members, coaches, volunteers, and anyone involved with the club.

2. Ensure Understanding

As the saying goes, "You can't manage what you can't measure," and this is especially true regarding data protection. Each Squash Club must understand the personal information it holds and is responsible for. To clarify this, every club should inventory the personal data it holds and examine it under the following headings:

- Why is it being held?
- How was it obtained?
- Why was it originally gathered?
- How long is it being retained?
- How secure is it?
- Is it shared with any third parties?

The primary source of personal information held by a Squash Club is its membership database, whether in paper form, on a spreadsheet, or within a specially designed Membership Management System. Special consideration must be given to paper membership forms and how they are managed once completed and received by the club. It is acceptable to collect and retain information on paper forms, provided the member is informed at the time of completion and consent is obtained. Completed forms must be stored securely in a specified location.

The same principles apply to any other system or database used to manage club membership. Technology supports are acceptable, but careful attention must be paid to data security and the use of third-party providers. These providers should be aware of GDPR compliance and able to advise on their compliance measures. Clubs using third-party systems should verify GDPR compliance with their providers.

Other likely categories of personal information held by Squash Clubs include:

- Information required for Garda vetting
- Summer camp or coaching applications

- Text or messaging systems
- Email lists or distribution groups
- Team sheets or training attendance lists
- Accident report forms
- Disciplinary reports
- Information captured on club websites

Each club should maintain a record of all personal data it controls.

3. Clear Communication

Individuals must be informed about why their data is being collected and who will have access to it before their data is obtained. Existing data protection laws require this, and the GDPR expands these requirements. Membership forms and other data collection forms must be updated to inform individuals of:

- The club's identity
- The reasons for collecting the information
- The uses of the information
- Who it will be shared with
- If it will be transferred outside the EU
- The legal basis for processing the information
- The retention period
- Members' rights to complain about GDPR implementation
- Other specific personal privacy rights under GDPR

For a membership form template, refer to the Irish Squash handbook emailed to all clubs. Contact info@irishsquash.com for a copy.

4. Ensure Personal Privacy Rights

The GDPR grants individuals certain rights that must be upheld by all data controllers, including Squash Clubs. These rights include:

- Access to all information held about an individual (Subject Access Request), to be provided within one month.
- Correction of inaccuracies
- Erasure of information
- Objection to direct marketing
- Restriction of data processing, including automated decision-making
- Data portability, enabling individuals to receive their information in a standard format to transfer to another provider

5. Obtain & Manage Consent

The GDPR mandates that individuals be informed of the use of their personal information, who will access it, where it will be stored, and how long it will be held. Consent must be freely given, specific, informed, and unambiguous. It must be a positive indication of agreement, not inferred through silence, pre-ticked boxes, or inactivity.

Consent must be verifiable, and data controllers must maintain an audit trail. For paper forms collecting personal information, the retention period should align with the need to demonstrate consent. For children, consent must be given by a parent or guardian, as existing Irish Squash policy supports.

Many clubs will need to update their membership forms to include and verify appropriate consents.

6. Report Data Breaches

Unauthorised access to personal data or data loss must be reported to the Data Protection Commissioner within 72 hours of identification. This applies to both paper and electronic information (unless encrypted or anonymized). If a breach may harm an individual (e.g., identity theft or confidentiality breach), the individual must also be informed. Clubs should have procedures to detect, report, and investigate data breaches.

Data breaches or potential breaches should not be ignored and must be investigated and reported as appropriate. Advice on data protection queries can be obtained by emailing the Data Protection Commissioner's office.

7. Ensure Privacy by Design

The GDPR requires that all significant new processes, initiatives, or projects consider and ensure GDPR compliance. This involves conducting a Data Protection Impact Assessment to understand the potential impact on individuals' privacy. Squash Clubs considering high-risk processing (e.g., new technology or CCTV installation) should conduct an assessment, involving relevant stakeholders to identify and mitigate privacy issues.

8. Identify Data Protection Officers

Each Squash Club should appoint someone to coordinate their data protection obligations. This includes identifying and recording data locations, ensuring consent is appropriately obtained and maintained, and overseeing overall data protection compliance.