IMPORTANT INFORMATION – "GDPR" Compliance 2018

What is GDPR????

- The General **Data Protection** Regulation (GDPR) will **come into force on the 25th May 2018**, replacing the existing data protection framework under the EU Data Protection Directive.
- It very clearly sets out the ways in which the privacy rights of every EU citizen must be protected and the ways in which a person's 'Personal Data' can and can't be used.
- It places the onus on the person or entity that collects a person's information (Data Controller) to comply with the legislation and to demonstrate compliance.
- It carries significant penalties for non-compliance.

What is Data Protection?

- Data Protection refers to legislation that is intended to:
  - Protect the right to privacy of individuals (all of us)
  - Ensure that personal information is used appropriately by third parties that may have it (Data Controllers)

Data Protection relates to any information that can be used to identify a natural person such as

- Name
- Date of Birth
- Address
- Phone Number
- Email address
- Membership Number
- IP Address
- Photographs etc

GDPR Timelines:

- GDPR is coming into effect on May 25th 2018.
- All data processing from that date will legally be required to comply with GDPR.
- There are consultations and working groups on-going within the EU and Member States to produce guidance on certain elements of the regulations.
- Recital 171 of GDPR makes allowance to bring 'non-GDPR' processing already underway into compliance within 2 years.
- If consent was already obtained in a manner consistent with GDPR, it is not necessary to obtain consent again.

Impacts on the GAA:

- GDPR places responsibilities on GAA units to comply and to demonstrate compliance.

  - Consent needs to be obtained and refreshed regularly.
  - Privacy statements need to be updated.
  - Information needs to be protected and accurate.
  - Specific locations of information must be known.
  - Subject Access Request must be facilitated (1 month).
  - Breaches must be reported within 72 hours.
  - Privacy by design and by default must be adopted.

- New procedures must be implemented to enable the above throughout the **lifecycle of the data**.

How to Comply:

The Data Protection Commissioner has issued a guide to compliance, consisting of 12 steps:

Step 1 – Awareness

- GDPR will benefit all of us, it will ensure that our Personal Information is protected.
- It will also ensure that, as a Data Controller, each GAA Club, County or Provincial Board will be accountable for how it collects, uses and stores Personal Information.
- Every Member should be aware of the changes that GDPR will bring and how that impacts them, either as a volunteer working on behalf of the club or as an individual Club Member.
- This awareness will also benefit all of us in our personal lives.
- Clubs should ensure that information relating to GDPR is made available to Committee Members, Club Members, Coaches, Volunteers or anyone who is in anyway involved with the Club.
- Information regarding Data Protection can be found on the GAA website http://www.gaa.ie/dataprotection.

Step 2 – Become Accountable

- It is imperative that each GAA Club understands exactly what Personal Information it holds and how it uses it.
- To ensure that this is clear, it is important that every club makes an inventory of the personal data that it holds and the processing activities undertaken.
- This Inventory or 'Processing activities log' should examine data under the following headings:
  - Why is it being held?
  - How was it obtained?
  - Why was it originally gathered?
  - How long is it being retained for?
  - How secure is it?
  - Is it shared with any third parties?
- All registered members' information is stored on the GAA's central Games Management System (Servasport) and responsibility for this information is jointly held by the GAA centrally.
- Other likely categories of Personal Information held by GAA Clubs will include:
  - Information required for Garda Vetting.
  - Cul Camp or other training camp applications.
  - Text or messaging systems.
  - Email lists or distribution groups
  - Teamsheets, training attendance lists
  - Information captured on club websites

Step 3 – Clear Communication

- It is required that individuals are aware of certain information before their data is obtained.
- Existing membership forms, and other forms used to collect data (e.g. Garda Vetting, Websites, etc.) must be updated to specifically tell individuals the following:
  - The club's identity.
  - The reasons for collecting the information.
  - The uses it will be put to.
  - Who it will be shared with.
  - If it's going to be transferred outside the EU.
  - The legal basis for processing the information.
  - How long it will be retained for.
  - The right of members to complain.
  - Whether it will be used for automated decision making.
  - Other specific personal privacy rights relevant under GDPR.

Step 4 – Personal Privacy Rights

- GDPR enshrines certain rights for individuals that must be supported by every Data Controller, including GAA Clubs.
- These rights include:
  - Subject Access.
  - To have inaccuracies corrected.
  - To have information erased.
  - To object to direct marketing.
  - To restrict processing of their information including automated decision making.
  - Data portability - Ability to receive all of their information in a standard format to move to another provider (more relevant for switching banks or utility providers than GAA Clubs but must be supported).

Step 5 – Subject Access Requests

- Under Data Protection, a person has always had the right to request access to **all** of the information held about them.
- This is called a Subject Access Request (SAR).
- Subject Access Requests must be completed within one month.
- Holding an accurate inventory of information will be a key enabler for completing SAR efficiently.
- Data has to be provided in a standard format.
- The person must also be informed of the relevant Retention Periods for the data held and their right to have inaccuracies corrected.

Step 6 – Legal Basis for Data Processing

- Processing of Personal Information can only occur when there is a legal basis for carrying it out.
- Legal Basis can be established where one of the following applies:
  - The person has given explicit **consent**.
  - Necessary for **performance of a contract**.
  - Compliance with a **Legal Obligation**.
  - To protect the **vital interests** of the person.
  - A task carried out in the **public interest**.
  - For the **legitimate interests** of the data controller.
- The legal basis for processing should be recorded.

Step 7 – Obtain & Manage Consent

- Individuals must be **informed of what their data is going to be used for, who will have access to it, where it will be stored and how long it will be held for**.
- They **must give their consent** for their data to be used.
- Consent must be **'freely given, specific, informed and unambiguous'**.
- Members **cannot be forced** into consent or **unaware** that they are giving consent.
- Obtaining consent requires a **positive indication of agreement** – it cannot be inferred through silence (not objecting), pre-ticked boxes or inactivity.
- Consent must be **'refreshed'** – It cannot be deemed as indefinite.
- Consent **must also be verifiable** – Data Controllers must be able to demonstrate that consent was given and an audit trail should be maintained.
- 'Legal Basis' can be used to process information in the absence of consent in certain, very specific, circumstances.
- It must be easily possible for a person to **withdraw their consent**.

Step 8 – Children's Data

- Under GDPR, children are not permitted to give consent for Data Processing.
- A child's Parent or Guardian must give consent on their behalf.
- Procedures must be in place to verify individual's ages (for juveniles).
- Existing GAA policy relating to Juvenile members already supports this legislative requirement.

Step 9 – Data Report Breaches

- If unauthorised access to Personal Data occurs or Personal Data is lost or stolen, this **must be notified** to the Data Protection Commissioner within 72 Hours of being identified.
- This is a requirement for all paper information and all electronic information (**unless the data is encrypted** or anonymised).
- If the breach is likely to cause harm to the individual (Identity Theft or breach of confidentiality) then the **individual must also be informed**.
- A procedure to detect, report and investigate data breaches should be in place.
- It is imperative that Data Breaches or possible Data Breaches are not ignored in the hope that no one will notice, they must be investigated and reported if appropriate to do so.
- Advice on data protection queries can be obtained on the gaa website http://www.gaa.ie/dataprotection or by emailing dataprotection@gaa.ie.

Step 10 – Data Protection Impact Assessments

- GDPR seeks to ensure that all significant new processes, initiatives or projects undertaken consider and ensure GDPR compliance.
- The concept of 'Privacy by Design and by Default' is a key theme within GDPR.
- This requires that a Data Protection Impact Assessment must be undertaken to understand the potential impact of that project /initiative on the privacy of individuals.
- GAA Clubs that are considering projects with 'high risk' processing (i.e. new technology) or installing CCTV should conduct a Data Privacy Impact Assessment.
- A Data Privacy Impact Assessment can be conducted by meeting relevant stakeholders, identifying potential privacy issues and agreeing ways to mitigate the risk of issues occurring.

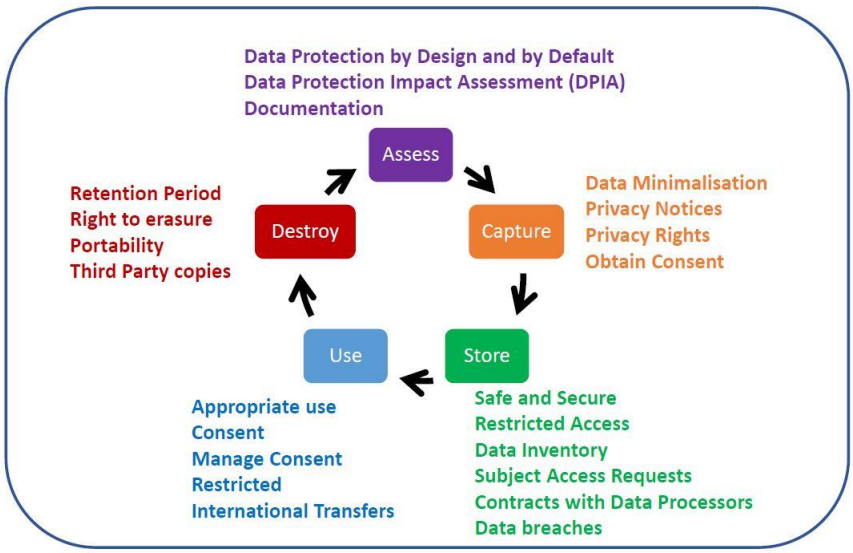
Step 11 – Data Protection Officers

- Every GAA Club should identify someone to coordinate their approach to meeting their Data Protection obligations.
- This will involve identifying and recording the specific locations where data is held in each club, ensuring that access to the data is controlled, ensuring that consent is obtained in the appropriate manner and maintained accordingly.
- The GAA centrally will have expertise available for any Data Protection queries that require additional / legal advice. Queries of this nature can be submitted to dataprotection@gaa.ie.

Step 12 – Internal Organisations

- GDPR includes a 'one-stop shop' provision for Organisations that operate in more than one jurisdiction.
- A Lead Supervisory Authority can be nominated.
- For the GAA this will be the Data Protection Commissioner, based in Portlaoise.

SUMMARY OF "GDPR" INFORMATION CYCLE



1) Capturing Information under GDPR

Capture

1. **Data Minimalisation** (Only ask for what is needed)
2. **Privacy Notices** (Clearly inform what, why, who and where)
3. **Privacy Rights** (state the persons rights under the legislation)
4. **Obtain Consent** (consent must be freely given and explicit for the purpose or purposes)

2) Storing Information under GDPR

Store

1. **Safe and Secure** (Information must be stored appropriately)
2. **Restricted Access** (Only authorised persons should have access to it)
3. **Data Inventory** (Information captured should be recorded)
4. **Subject Access Requests** (Must be in a position to provide ALL information held)
5. **Contracts with Data Processors** (Any third parties must have GDPR contracts in place)
6. **Data Breaches** (Processes to detect, report and investigate Data Breaches must be in place)

3) Use of Information under GDPR

Use

1. **Appropriate use** (Must be for the purpose(s) originally stated)
2. **Consent** (Must have person's consent or a lawful basis for processing it)
3. **Manage Consent** (Individuals have the right to revoke consent for part or all of the processing, this must be managed)
4. **Restricted** (Profiling or automated decision making are restricted)
5. **International Transfers** (Any processing that occurs outside EU must have been communicated to person at time of data capture)

4) Destruction of Information under GDPR

Destroy

1. **Retention Period** (Must destroyed after its useful retention period has expired)
2. **Right to erasure** (Must be erased upon request from person)
3. **Portability** (Must be provided in standard format)
4. **Third Party Copies** (All copies of information must be deleted including those held by third parties)

5) Assessment of Relevant Projects – Ensuring Privacy by Design

Assess

1. **Data Protection by Design and by Default** (All relevant projects or initiatives must consider impacts on privacy).
2. **Data Protection Impact Assessment (DPIA)** (Must be conducted for new technology, for profiling or for large scale processing).
3. **Documentation** (Decisions and rationale for decisions around Data Protection should be documented)

Checklists of Things to Do:

- Ensure Awareness within club
- Ensure Privacy by Design & Default
- Create Inventory of Data Processing Activities
- Review Access to Personal Information
  - Evaluate who has access to personal data on the GMS (Servasport) and ensure they are authorised.
  - Evaluate any other systems that hold member information for appropriate access.
- Ensure any third parties have provided assurance on GDPR compliance.
- Ensure Paper Forms are stored in known and safe locations.
- Ensure any Laptops holding data are encrypted.
- Ensure any spreadsheets are password protected.
- Ensure a SAR process is in place.
- Ensure a process to report data breaches is in place.
- Ensure documentation is in place.
- Ensure BCC Function on email is used.
- Leverage OneDrive as a mechanism to keep electronic data secure.

Supports Available:

The GAA Centrally will provide:

- Access to Data Protection Officer.
- GDPR compliant processes.
- GDPR compliant templates.
- Tools to support compliance
  a) GAA Membership Mobile Phone App (Available from 23rd January 2018)
  - Registration (Personal Information – Secure, accurate up to date)
  - Payments
  - Communications (Consent)
  - Reduction in Paper Records

  b) One Drive & Office 365
  - Use of Office 365 Accounts (@gaa.ie email addresses) will support GDPR
  - OneDrive can be used to secured store information
  - Access to OneDrive can be controlled
  - Microsoft Office Products (Word / Excel) can be password protected to ensure security
- Further Information Online
  - Relevant information is available on website GAA.ie/dataprotection
  - On-line course available
  - Multiple choice online quiz included to test your knowledge

As a Result of the upcoming GDPR changes the following Privacy Notice has been incorporated into the Moynalvey GFC Membership form which is available for download from www.moynalveygfc.ie

"The following Privacy Information is being provided to you as outlined in the General Data Protection Regulation. It is intended to inform you of how the Personal Information provided on this form will be used, by whom and for what purposes. If you are unclear on any aspect of this form, or want any further information, please contact the GAA's Data Protection Officer (01 8658600 or dataprotection@gaa.ie

Who is the data controller?
Moynalvey GFC is the Data Controller of the Personal Data and contact details for the Club are as follows:
Moynalvey GFC, Kilmore Park, Moynalvey, Summerhill, Co. Meath – email: secretary.moynalvey.meath@gaa.ie

Who is the Data Protection Officer for the GAA and the Club?
Moynalvey GFC Data Protection Officer is Paul Greene. You can contact Paul by e-mailing pro.moynalvey.meath@gaa.ie. The GAA Data Protection Officer is Gearoid O'Maolmhicil. You can contact Gearoid at dataprotection@gaa.ie or 01 8658600. If you have any questions or wish to make any request in relation to your personal data.

What is the purpose of processing my Personal Data?
The purpose for processing your Personal Data is that it is necessary for the performance of a contract in order to register and maintain your membership with the Club and the GAA.
The purpose is also to keep you informed of GAA events and fundraisers. We will only use your personal data for this second purpose if you have provided your explicit consent for this by ticking the boxes on this form and signed below those boxes.

Will anyone else receive a copy of my Personal Data?
Your Personal Data can be accessed by certain members of Moynalvey GFC Executive Committee. This will be done in accordance with our data protection policy only.
In the event of an injury or insurance claim, details of your claim which will include your Personal Data will be passed to the GAA's Insurance underwriters, Willis Insurance, Elm Park, Merrion Road, Dublin 4, Ireland.

Where is your Personal Data stored?
Your data will be stored electronically on the GAA Membership Database which is provided by Servasport Ltd, 11th Floor, Causeway Tower, 9A James Street South, Belfast, BT2 8DN.

Who is Servasport Limited?
Servasport Limited is a "data processor" who hosts the database on which your information is stored. The GAA have a contract in place with Servasport Limited to ensure your Personal Data is stored safely and securely.

How long will your Personal Data be stored for?
Your Personal Data will be held for the duration of your Membership and it will be deleted by us in the event that you resign your Membership or you are expelled in accordance with the Official Guide. However we may retain your Personal Data after your Membership ceases if we decide that it is strictly necessary to do so in the circumstances.

How can I obtain a copy of the Personal Data held by the Club/GAA?
You have the right to request a copy of all of your Personal Data and can do so by contacting us. This information will be provided to you within one month.

What are my privacy rights relating to my Personal Data?
You have the right to have your Personal Data updated, rectified, or deleted if you so wish. You have the right to object to your Personal Data being processed and to withdraw your consent to processing - You can do so by contacting us.

Where can I get further information?
Further information regarding your rights can be obtained through the **Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois**, or on the website www.dataprotection.ie

How do I make a complaint or report a breach?
Should you wish to make a **complaint or report a breach** under in relation to your Personal Data, you can do so by emailing the Office of the Data Protection Commissioner using the following email address: info@dataprotection.ie