

GDPR

What your club needs to know and do



Data Protection 2018

Introduction

There are some significant changes to Data Protection legislation from May 25th 2018. The General Data Protection Regulation (GDPR) and the Irish Data Protection Bill 2018 will have an impact on how the GAA, at all levels, engages with its members.

It is important that every GAA Club, and indeed every member, is aware of how these changes in the law will affect the ways in which members' personal information can be collected and used for GAA Purposes.

The following document describes some of the practical changes that need to be made to ensure compliance with the new legislation. It comprises three distinct sections:

- 1 - General information on GDPR
- 2 - Specific actions required to be taken by GAA Clubs
- 3 - Supports available and FAQs



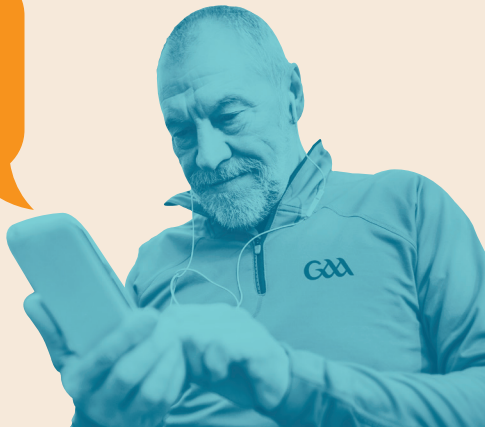


Why do I have to accept cookies?



Opt -out?

Text STOP to 57117



How can I identify the information our club holds that is relevant for Data Protection Legislation, I'm not even sure what Data Protection is?

What is Data Protection?

Data Protection legislation is intended to protect the right to privacy of individuals and seeks to ensure that Personal Information is used appropriately by organisations that may have it (Data Controllers/Data Processors).

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

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

There are other categories of information defined as Special Categories of Personal Data which require more stringent measures of protection and these include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Processing of genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation.

Children's data and data relating to criminal convictions or offences also require more stringent levels of protection.

What is GDPR?

The General Data Protection Regulation (GDPR) is new EU legislation that comes into effect on May 25th 2018.

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 uses a person's information (Data Controller/Data Processor) to comply with the legislation and to demonstrate compliance.

What does Data Protection Legislation mean for me?

The legislation sets out rules about how this information (Personal Data) can be obtained, how it can be used and how it is stored.

Every person must give their consent for their data to be collected and processed for a specific purpose which must be communicated to them at the time the data is obtained.

Data must be kept safe and secure and must be kept accurate and up to date.

An Individual can request a copy of all of the personal information held about them (this is called a Subject Access Request) and must be allowed to have all of their data deleted or returned to them, if they so wish.

GDPR Principles



Seven Principles of GDPR

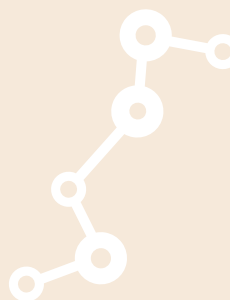
1. Lawfulness, Fairness, Transparency
2. Purpose Limitation (Use only for one or more specified purposes)
3. Data Minimisation (Collect only the amount of data required for the specified purpose(s))
4. Accuracy (Ensure data is kept up to date, accurate and complete)
5. Storage Limitation (Kept for no longer than necessary for the specified purpose(s))
6. Integrity and Confidentiality (Processed ensuring appropriate security of data)
7. Accountability (Essential not only to be compliant, but to be able to demonstrate compliance)

Penalties for Non-Compliance

Fines can be imposed on organisations found to be in breach of GDPR. The level of the fines depend on the subject matter and gravity of the breach with maximum fines resting at €20 million/4% of global annual turnover (whichever is higher).

Of potentially more importance to GAA Clubs, individuals have the right to sue organisations for misuse of their Personal Data under the GDPR. Therefore it is imperative to communicate with individuals in a timely manner in relation to their Personal Data, e.g. responding to Subject Access Requests within the allotted timeframe.

The Office of the Data Protection Commissioner can order organisations to cease processing Personal Data if the organisation is misusing individuals' information.



Ensuring Compliance



It is imperative that every GAA club understands the principles of Data Protection and how the upcoming changes in legislation will affect them. The following are key steps clubs should take.

Awareness

GDPR will benefit all of us, it will ensure that our Personal Information is protected from misuse by any organisation. 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 information about the GAA members under their remit.

It is critically important that every member is 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 as GDPR also relates to Banks, Insurance Companies, Utility providers, On-line Marketing etc. 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>

Clear Communication

As noted above, it is required that individuals are made aware of certain information such as why their data is being collected and who will have access to it, before their data is obtained. Under existing Data Protection law, it has always been a requirement to provide some of this information to individuals. GDPR builds on this requirement and expands the information that must be given to Individuals in advance of collecting and using their data.

Existing membership forms, and other forms used to collect data (e.g. Garda Vetting) must be updated to specifically tell individuals the following:

- The Clubs identity
- The reasons for collecting the information
- The uses it will be put to
- Who it will be shared with (e.g. third parties)
- If it is 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 if they are unhappy with the club's implementation of GDPR
- Other specific personal privacy rights relevant under GDPR (See next page)

The GAA centrally has obtained legal advice and the Official Membership Forms in the Official Guide are GDPR compliant. These can be downloaded from the GAA website

Useful resources such as Membership Forms, GDPR Compliant templates and guidance on data protection can be found on the GAA website: www.gaa.ie/dataprotection



Ensure Personal Privacy Rights

GDPR enshrines certain rights for individuals that must be supported by every organisation involved in the processing of Personal Data, including GAA Clubs. These rights include:

- Access to information held about them (Subject Access Request)
- To have inaccuracies corrected
- To have information erased in certain circumstances
- 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 (i.e. to switch utility provider)

The Office 365 logo is displayed in orange text next to the Office 365 icon, which is a white square with a red 'O' shape inside, all set against a white cloud-like background.

What supports are available?

On-line Materials

Information relating to Data Protection and GDPR is available on the Data Protection Commissioner's website at the following URL: <http://www.dataprotection.ie>

Additional information and how data protection specifically impacts on the GAA and supporting templates, forms and process documentation is available on the GAA website www.gaa.ie/dataprotection. This information is also shared via OneDrive with all Club Officers who use their GAA Office 365 accounts. Guidance on how to access OneDrive is included later in this document.

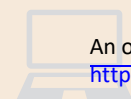
Data Protection Officer

The GAA have provided access to a Data Protection Officer to all Clubs. Any questions, queries or issues in relation to Data Protection should be emailed to dataprotection@gaa.ie.

Training

Data Protection Seminars for Clubs have been held in Croke Park and in each province going through the topic in detail. A range of materials (including Processes and templates) were provided to Clubs at those meetings. These materials can be accessed at www.gaa.ie/dataprotection and on the OneDrive GDPR Repository for Clubs. Further training is planned and will be communicated through the GAA Club Newsletter.

An online module to train club administrators, registrars, club executive committee and members is available at <https://learning.gaa.ie/courses/dataprotection>



Specific Actions for Clubs





Specific Actions for Clubs



Much of what is required under GDPR is already in place in many clubs. However, there are some specific new actions that must be completed in the new regime. These are described below:

1 Designate responsibility

Every GAA Club should identify someone or a group of people to coordinate their approach to meeting their Data Protection obligations. Their tasks will include identifying and recording the specific locations where data is held in each club, ensuring that consent is obtained in the appropriate manner and maintained accordingly. The GAA centrally has a Data Protection Officer available to Clubs to provide assistance in relation to any data protection questions, queries or issues. Queries of this nature can be submitted to dataprotection@gaa.ie

2 Create a Personal Data Inventory

As the saying goes, 'You can't manage what you can't measure' and this is especially true regarding Data Protection. It is imperative that each GAA Club understands exactly what Personal Information it holds (and is responsible for). To ensure this is clear, it is important that every club makes an inventory or record of processing activities of the personal data that it holds. A template is available on the OneDrive GDPR repository for Clubs.

Obviously, the primary source of Personal Information held by a GAA Club is its Membership database. 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.

Specific consideration must also be given to Paper Membership forms and how these are managed once they have been completed and received by the club. It is vitally important that any completed forms are stored securely in a specified location.

The same logic should be applied to any other system or database used to assist a club when managing its membership. It is OK to use third party technology supports in this way but careful attention must be paid to how and where data is stored (it must be secure and should be encrypted) and individuals must be informed if a third party is being used to provide a system for this purpose.

Other likely categories of Personal Information held by GAA Clubs will include:

- Information required for Garda Vetting
- Cúl Camp or other training camp applications
- Text or messaging systems
- Email lists or distribution groups
- Teamsheets, training attendance lists
- Information captured on club websites

There may also be others, depending on individual clubs, and it is important that each club has a record of all of the Personal Data that it 'controls'. An example of what a Club Inventory could look like is available on the OneDrive GDPR repository for Clubs.

3 Third Parties

If your club is using a third-party system (Data Processor), the Club is obliged to ensure the third party is GDPR compliant. A contract or agreement relating to data protection responsibilities between the Club and the third party should be in place in order to demonstrate this compliance. Most of the third-party providers of these kinds of systems (online registration, text messaging, fundraising) are well aware of GDPR and will be able to advise on how they are ensuring compliance.

A Controller and Processor should enter into a Data Processing Contract which must, at a minimum, contain the following details:

- The subject matter, duration, nature and purpose of the data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed;
- The obligations and rights of the Controller



A Data Processing Contract should also contain the following mandatory provisions:

- 1 - That the Processor will only process personal data received from the Controller on documented instructions of the Controller (unless required by law to process personal data without such instructions) including in respect of international data transfers;
- 2 - That the Processor ensures that any person(s) processing personal data is subject to a duty of confidentiality;
- 3 - That the Processor takes all measures required relating to Security of Processing including but not limited to implementing appropriate technical and organisational measures to protect personal data received from the Controller;
- 4 - That the Processor obtains either a prior specific authorisation or general written authorisation for any sub-processors the Processor may engage to process the personal data received from the Controller. The Processor must further ensure that where a general written authorisation to the Processor engaging sub-processors is obtained, the Controller has the opportunity to object in advance to each individual sub-Processor to be appointed by the Processor;
- 5 - That any sub-processors engaged by the Processor are subject to the same data protection obligations as the Processor and that the Processor remains directly liable to the Controller for the performance of a sub-processor's data protection obligations;
- 6 - That the Processor assists the Controller by appropriate technical and organisational measures to respond to data subject rights' requests under the GDPR;
- 7 - That the Processor assists the Controller to ensure its compliance with obligations under the GDPR in relation to security of data processing, notification of data breaches, and data protection impact assessments;
- 8 - That, at the end of the data processing by the Processor the Processor deletes or returns the personal data received from the Controller; and
- 9 - That the Processor makes available to the Controller all information necessary and that the Processor allows for and contributes to audits conducted by the Controller or a third party on the Controller's behalf.



4 Membership Forms

The Membership Forms published in the GAA Official Guide are GDPR compliant and all Clubs should be using the Official Membership Forms as a template in order to ensure compliance. The Official Membership Forms contain a privacy notice which outlines the information which is required to be provided to individuals prior to the collection of their personal data together with appropriate consent mechanisms.

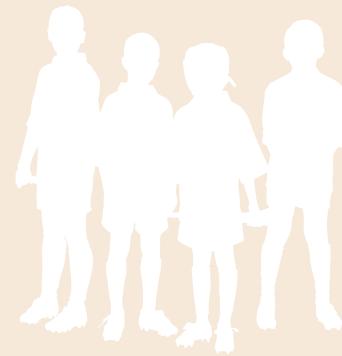
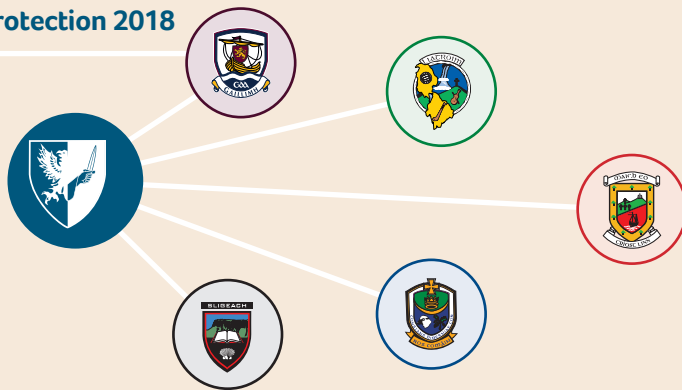
Official Adult, Youth and Child Membership Forms are available in the GAA Official Guide and on the GAA website www.gaa.ie/dataprotection

5 Consent

GDPR is very clear that an individual must be informed of what their personal information 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. In certain circumstances, they must give their consent for their data to be used. Consent must be 'freely given, specific, informed and unambiguous'. Consent cannot be bundled, i.e. "I consent to my information being used to notify me about my order and for marketing". Therefore, separate consent for each purpose must be obtained. 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 also be verifiable – Data Controllers must be able to demonstrate that consent was given and an audit trail should be maintained

Note: Where paper forms are used to collect personal information (e.g. Membership applications), the retention period (how long its kept for) of the form, or relevant portion of the form, should align with the need to demonstrate consent. Consent is not deemed to be indefinite and should be refreshed at least every two years, therefore the retention period of the form should be maximum two years. If consent is refreshed every year (i.e. a new form signed every year) the retention period for forms should be one year.



Under GDPR, children are not permitted to give consent for Data Processing. A child’s Parent or Guardian must give consent on their behalf. Existing GAA policy relating to Juvenile members already supports this legislative requirement.

If Clubs wish to publish contact details of individuals on their website, this is OK to do, once the individual has given their consent for their information to be published in this manner. An example of a consent form which may be utilised by Clubs to capture consent such as this is available on the OneDrive GDPR Repository for Clubs.

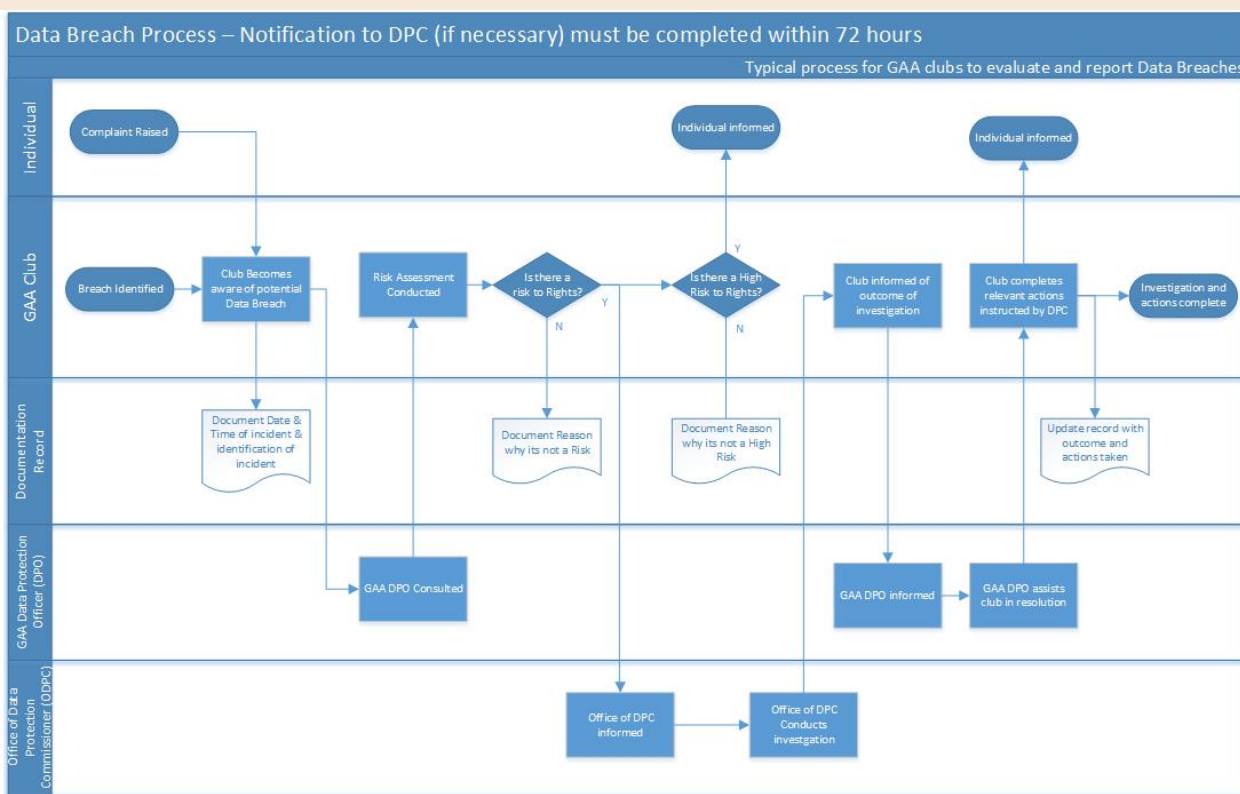
If the breach is likely to cause harm to the individual (Identity Theft or breach of confidentiality) then the individual must also be informed. A procedure to detect, report and investigate data breaches should be in place.

A Data Breach Process is available at www.gaa.ie/dataprotection and on the OneDrive GDPR Repository for Clubs. 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 necessary. If a Data Breach or suspected Data Breach is identified within a Club, advice on the procedure to follow including any reporting obligations can be obtained from the GAA’s Data Protection Officer at dataprotection@gaa.ie.

6 Data Breach Process

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).

Note: The 72-hour deadline for notification to the Data Protection Commissioner applies irrespective of any steps being taken to understand the causes of the breach.



8 Subject Access Requests Process

Subject Access Requests or SARs allow for any member to request a copy of information held about them. This must be provided in paper format or in a standard electronic format within thirty days. It is no longer allowable to charge for responding to SARs.

The GAA's Subject Access Request process is available on at www.gaa.ie/dataprotection and on the OneDrive GDPR Repository for Clubs.

It is of utmost importance that Subject Access Requests are responded to and dealt with within the allocated time frame. If a Subject Access Request is received by a Club, guidance on the procedure to deal with same can be obtained from the GAA's Data Protection Officer at dataprotection@gaa.ie

Note: Maintaining the Inventory of Personal Information outlined above will be a critical enabler for processing Subject Access Requests in a timely manner.

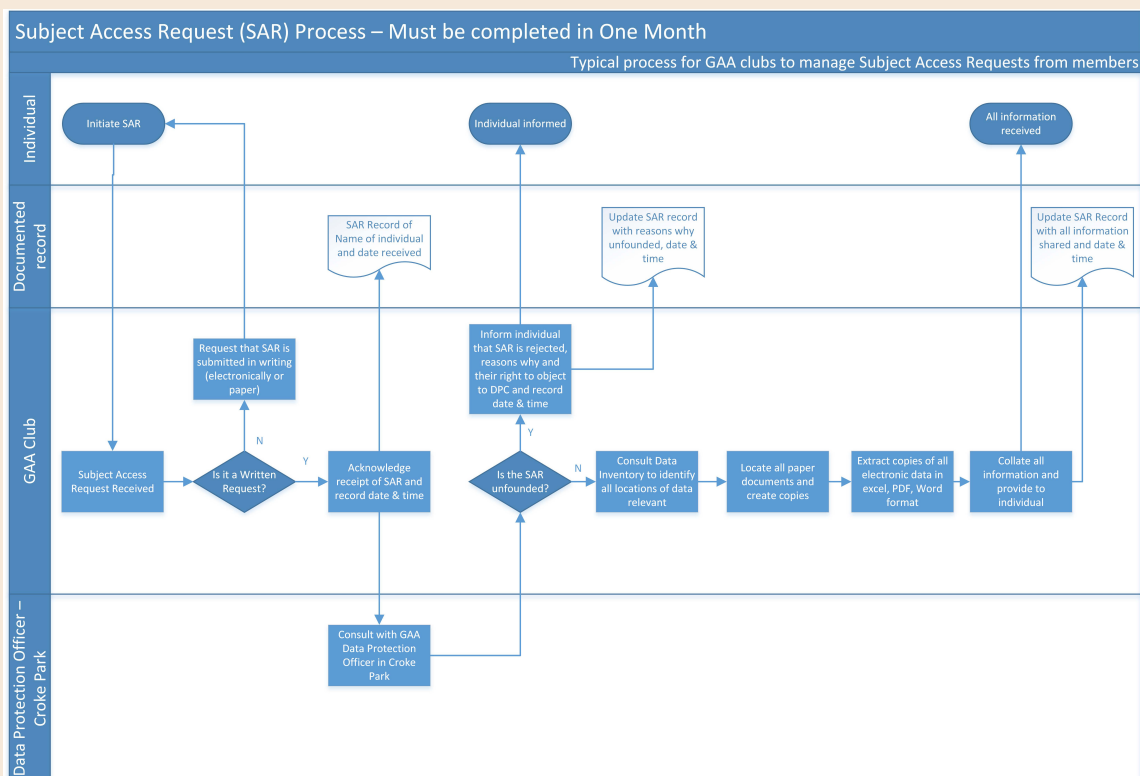
9 Communications

It is critically important that the wishes of individuals regarding communications sent to them are respected. Consent to contact must be recorded and maintained and if an individual has not given consent to receive communications, they must not be contacted.

Enhancements have been made to GAA systems to facilitate compliance with GDPR using technology, including the GAA App and Membership system. These allow GAA Club members to register and update their details on-line, thus making management of consent easier for clubs and reducing the amount of paper records.

The App also includes a messaging functionality to allow Clubs to communicate with their members through the App which is a GDPR compliant messaging service. The GAA centrally has a contract in place with Servasport governing the GAA App.

Clubs may also choose to utilise third parties to communicate with members, however, if Clubs choose to do so, the steps included above in relation to Third Parties must be adhered to.

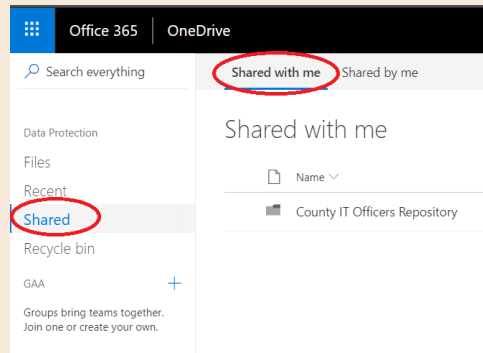
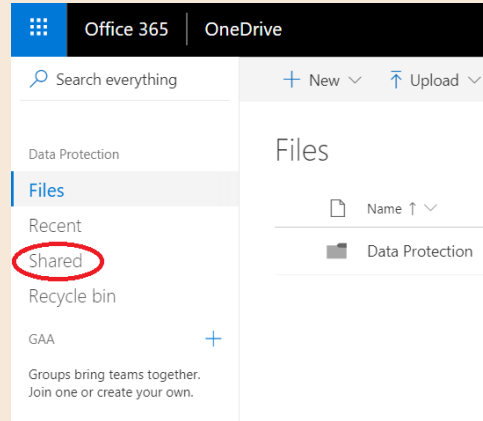
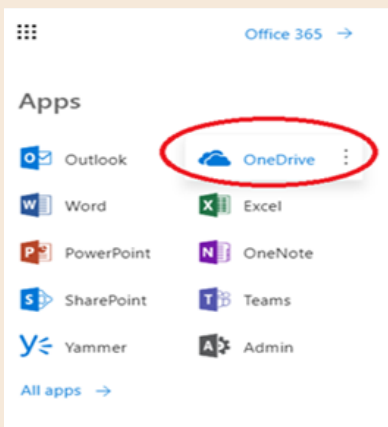
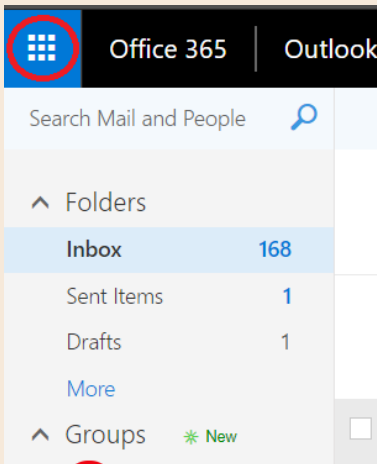


10 Secure Storage

All Personal Data held by Clubs, whether in paper form or electronic should be stored safely and securely. Paper copies of Personal Data should be stored in locked cabinets and securely shredded once they have fulfilled their purpose. Electronic copies of Personal Data should be password protected and encrypted. All Microsoft products (Word, Excel etc.) can be password protected by clicking 'File' in the top left corner and 'Protect Document'.

Microsoft Office 365 will assist with GDPR compliance. Office 365 emails (@gaa.ie) where available should be used. Every Club has access to 4 @gaa.ie email addresses. If your Club is not currently using one or a number of those allocated please let us know at dataprotection@gaa.ie.

OneDrive within Microsoft Office 365 can be used to store information securely. Access to OneDrive is available to all with a @gaa.ie email address and can be accessed with the same username and password utilised for @gaa.ie email addresses. OneDrive can be accessed by following the steps.



OneDrive is also a secure mechanism to share information in a secure and controlled manner. The GAA has a contract in place which allows us to control the data in a manner that is compliant with GDPR (i.e. the location of data is known and it can be deleted or copies obtained if requested).

Clubs are advised to use OneDrive to share content within their clubs rather than attaching files via email or using third party file sharing sites.



11 Privacy by Design

GDPR seeks to ensure that all significant new processes, initiatives or projects undertaken consider and ensure GDPR compliance from the outset of the project. This requires a **Data Protection Impact Assessment** to be undertaken to understand the potential impact of that project / initiative on the privacy of individuals in certain circumstances. GAA Clubs that are considering projects with 'high risk' processing (i.e. new technology) or installing CCTV should conduct a Data Privacy Impact Assessment by meeting relevant stakeholders, identifying potential privacy issues and agreeing ways to mitigate the risk of issues occurring. A sample Data Protection Impact Assessment is available at www.gaa.ie/dataprotection and on the OneDrive GDPR Repository for Clubs. A Data Protection Impact Assessment should follow the steps below:



12 Review Access

Access to all Personal Data held by the Club should be reviewed. This is to include all systems utilised by the Club, such as the Games Management System, Office365 and any other systems used. It should also include physical files that contain Personal Data.

Clubs should ensure that previous members of the Executive do not have access to key systems unless their current role within the Club specifically requires such access. Clubs should carry out a review of access to their Membership records contained on the Games Management System by following the steps outlined later in this document to ensure only the appropriate people have access to the system. A similar review should be carried out on all other systems Clubs may use.

13 If In Doubt, Ask!

Complying with Data Protection legislation and GDPR can be daunting and it will take some time before all GAA volunteers are fully comfortable with the changes that the new regulations have brought. There will always be questions regarding specific processes used in Clubs and the simple advice is 'if in doubt, please ask'.

The GAA has provided a Data Protection Officer to assist Clubs with their data protection obligations. If any queries in relation to data protection arise please email dataprotection@gaa.ie.

Supports Available



Obtaining Consent to contact your Club Members

It is important that your club members' preferences regarding Communications are respected. They must give their consent, by ticking a relevant consent box, before being added to the club's communication lists. This consent should be recorded during the Annual Club Membership process and it is necessary to 'refresh' consent at least every two years – having a signed form with the relevant boxes ticked from five years ago is not suffice.

Paper Membership Forms

If your club uses Paper Membership Forms, you must use the format provided in the GAA Official Guide which includes the relevant consent options and the correct Privacy Notices and other Data Protection relevant clauses. Using this form will allow your club to capture consent in the correct manner. It is obviously critically important that the wishes expressed by your members on their completed forms are reflected in your club's communications – if someone does not give their consent to receive communications, you **MUST** not include them in emails, text or other message distribution lists

Communications issued should include an opt-out option and, again, changes to preferences expressed by members through these opt-out mechanisms must be reflected in your club's distribution lists.

Online Membership

Many clubs choose to offer their members the option to complete their membership subscription using on-line tools. This is perfectly fine under GDPR as long as the appropriate information is provided to your members during the process. The correct Privacy Notices must be displayed and consent must be captured correctly. Any consent options cannot be pre-ticked and membership cannot be conditional on providing consent to receive 'marketing' emails.

As is the case with paper forms, it is critical that the wishes expressed by your members on their completed forms are reflected in your clubs communications – if someone does not give their consent to receive communications, you **MUST** not include them in emails, text or other message distribution lists.

I have read the important Data Protection information on the reverse of this form and have given my consent, by ticking the boxes and signing below, for my information to be used as follows:

(Please tick as appropriate)

- (1) To provide me with updates regarding Club activities such as matches, meetings and club events
- (2) To provide me with details of Club fundraising activities including Lotto, social occasions, ticket sales etc

Managing Consent

Once a member provides their consent it must be managed appropriately. It must be easy for them to decide to opt-out of receiving communications and they must be given the opportunity to 'refresh' their consent regularly. In the GAA, members must be given the opportunity to refresh their consent at least every two years. This means that they must sign a new paper form at least every two years or, if registering on-line, must be given the opportunity to change their consent if they wish.



Tools to help manage consent

Obtaining and managing consent is a complex and onerous task for clubs to undertake and, in order to support this, a number of modifications and enhancements have been made to the GAA systems as follows:

Games Management System (Servasport)

Recording Communications Preferences

Every individual Membership record can be updated to include their individual Communications Preferences. This can be done logging onto the Games Management System, identifying the relevant member and selecting the Communications Preferences Tab within their Membership record as shown in the image below.

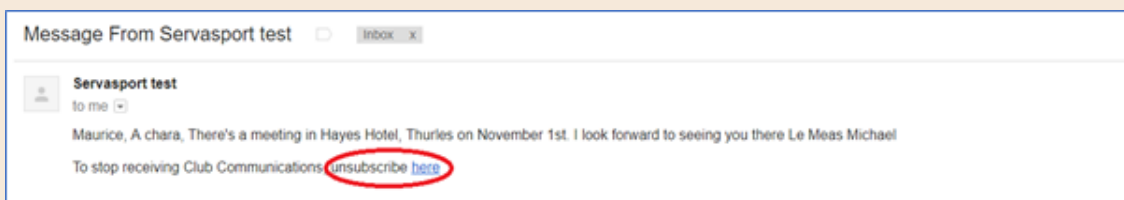
This will then provide the opportunity to record the Member's preferences against two categories of message:

- 1. Club Communications**
This option allows a member to consent to receive communications regarding Club activities including matches, training, notifications of meetings and / or the AGM, membership renewals, community announcements etc.
- 2. Additional Club Communications**
This option allows a member to consent to receive communications regarding Club Fundraising Activities including the club lotto, fundraising draws, social events, the club dinner dance, tickets and club merchandise.

These message categories allows the member to decide that, for example, they want to be informed when the U-12's are training but they don't want to receive communications about the Club Lotto. The second image below shows this.

Opting out of emails received

Messages received through the Games Management System include an opt-out link in the footer of the email which allows an individual recipient to stop receiving messages





GAA Mobile App

To help with GDPR Compliance (and general efficiencies for clubs) the GAA has developed a Mobile App which provides valuable functionality to both Members and Club Officials.

It provides clubs with the ability to allow their members to

- 1 - Login using their Club specific credentials
- 2 - Maintain / edit their Personal Information in a secure manner
- 3 - Review Club Privacy Notices and Privacy Right statements
- 4 - Give / revoke consent for club communications
- 5 - Receive Club communications in an auditable and controlled manner
- 6 - It also supports on-line payments of club memberships at registration time
- 7 - It helps clubs to reduce the risk associated with Paper
It removes the burden on administrators of keeping data up-to-date.
- 8 - It removes the need for administrators to manage consent
- 9 - It provides a free, controlled mechanism for Club communications

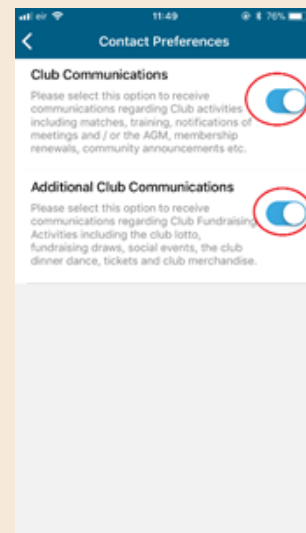
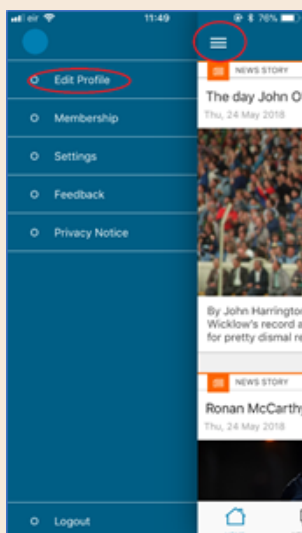
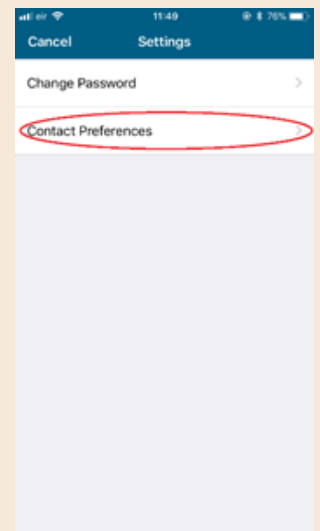
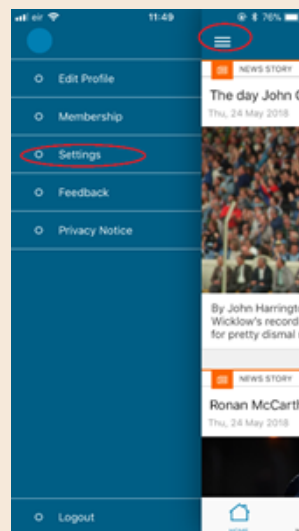
Keeping data accurate and up to date

There is a requirement under GDPR to keep data accurate and up to date. If paper membership forms are received on an annual basis, the data should be reviewed and any changes (i.e. address, contact details) reflected in the Registration / Games Management System.

Using the GAA App will allow members to edit their own contact details on a pro-active basis. They simply select the Edit Profile option from the menu and make the necessary edits to their profile – this is automatically reflected in the Registration system.

Recording Communications Preferences

Any member who has logged into the App can manage their own Communications preferences at any time. They can choose to receive communications or not and their preferences are reflected in the Club's distribution list (if using the communications module of the Games Management System). This means that any member who is using the GAA App can manage their own contact permissions and /or revoke their consent without any intervention from the Club.





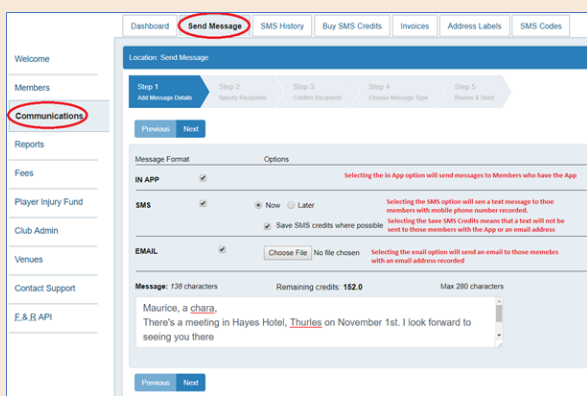
Sending Messages through the Games Management System (Servasport)

Managing communications preferences and sending the correct communications to the correct groups of people is critical to complying with GDPR. The functionality within the GAA's Games Management System (Servasport) has been enhanced to help clubs comply.

Sending messages from the system is simple and straightforward with a single interface to communicate with members via email, SMS or through the new GAA App. There are a number of steps to send messages:

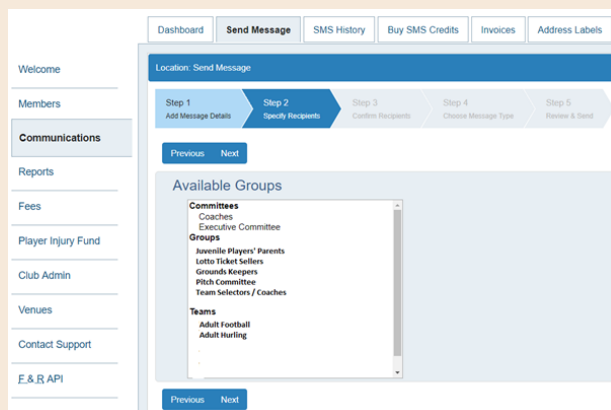
1. Determine the preferred communication channel

- IN APP – this option will send a free message to those members within the club with the mobile App installed.
- SMS – this option will send a text message to any member with a mobile phone number recorded on the system. SMS messages incur a cost from the providers and to help minimise these costs, the option to 'save SMS credits where possible' is provided. This means that a text will only be sent if none of the other free channels are available
- Email – this option will send an email to any member with an email address recorded in the system. (emails do include the Opt-out links in the email footer)



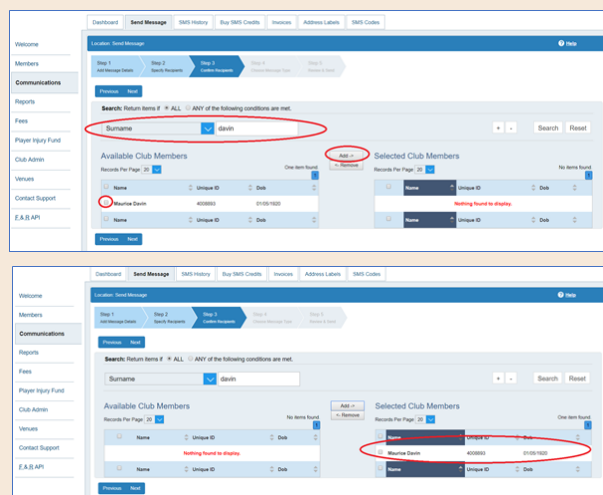
2. Specify Recipients

It is possible to create groups for communications purposes (i.e. the executive committee, or the parents of the u-10's or the Lotto Ticket Sellers) and broadcast the message to all in one go. Groups that are available can be selected at this step or simply clicking next will allow users to be added individually



3. Confirm Recipients

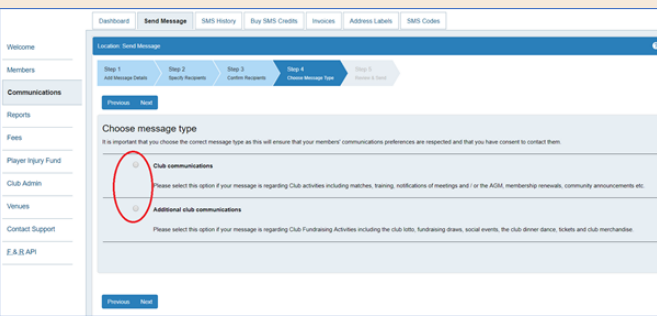
If a group had been selected, the relevant members would be shown on the right hand side below, but as none were selected in this example, it is possible to search for a member, select their record and add it to the recipients list.





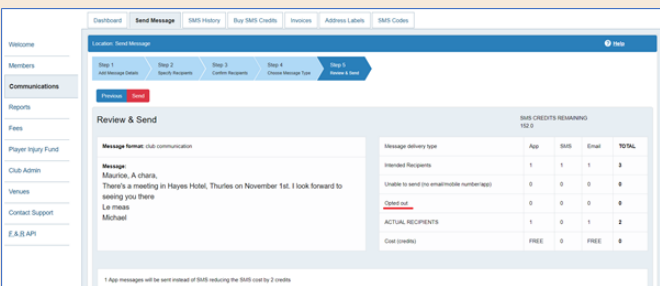
4. Choose Message Types

It is possible to categorise the message as either Club Communications or Additional Club Communications. It is important that this is done correctly as it allows the club to respect the wishes of their members from a communications perspective.



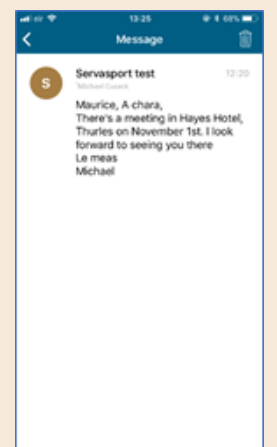
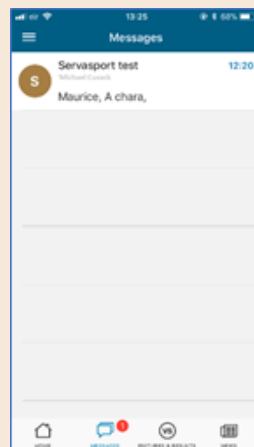
5. Review & Send

Before the communication is issued, there is an opportunity to review the messages and to amend if necessary. The numbers of people who receive the message and by what communication method is also displayed as are the number of who didn't receive the message because their phone number or email address wasn't present. The number of people who didn't receive the message because they have opted out for that particular type of communication is also displayed.



Receiving Messages through the GAA App

Once logged into the GAA App, the individual member has access to in-app messaging functionality. New messages are identified with the standard new message icons and all messages are displayed in the message tab, as shown below.



FAQs

1) Do Clubs require consent to publish photographs of members (including children) online?

Yes. Prior to photographs of any member being published on the Club's website or social media, the Club must be sure it has the appropriate consent captured for the member. Appropriate consent mechanisms are included in the Official Membership Forms. Clubs should now use the Official Membership Forms going forward which will ensure consent is captured in a GDPR compliant manner. In relation to photographs of children, the Child Membership Form requires parental consent as is GAA procedure. Official Membership Forms can be access in the Official Guide, on the GDPR Repository for Clubs or at www.gaa.ie/dataprotection.

At Club events, such as medal presentations etc., if photographs are being taken of the crowd, the Club should inform attendees prior to the photo(s) being taken to allow attendees to choose whether they wish to be in such photograph(s) or not.

2) How long is consent valid for?

If consent is being used by a Club as the legal basis for processing an individual's information (e.g. consent for photographs, for reminders about the lotto etc.), the Club must ensure it provides the individuals with the opportunity to refresh such consent on a regular basis. Consent cannot be deemed to be indefinite. Each time consent is captured, the Club should allow members an opportunity every 2 years to refresh such consent.

3) Is the GAA App an alternative communication method to Whatsapp?

Yes. The newly updated GAA App which is available for download on both iOS and Android encapsulates a messaging functionality within the App whereby the Club can communicate with its members via free in-app messages in a GDPR compliant manner. The GAA centrally has a contract in place with Servasport in relation to the App to ensure GDPR compliance. Clubs can set up groups within the App (e.g. lotto, senior hurlers etc.) and send communications based on the groups. In development at the moment is also the functionality for coaches to utilise the GAA App as a messaging system and Clubs will be updated once this functionality is enabled.

4) Do Clubs require a Data Protection Officer?

No. Clubs should identify a person/group designated with responsibility for compliance with data protection. The role, requirements and responsibility of a Data Protection Officer are specifically referred to in legislation. Individual GAA Clubs do not require a Data Protection Officer. The GAA centrally has provided access to a Data Protection Officer for Clubs and the GAA's DPO can be contacted at dataprotection@gaa.ie for any questions, queries, issues or concerns Clubs may have in relation to data protection.

5) Should Clubs collect medical information on membership forms?

Medical information should not be included on membership forms. A key principle of the GDPR is the principle of data minimisation, whereby only the personal data required for the purpose it is being collected for should be collected. For example, if buying a pair of shoes online, the order form should not request your occupation. Medical information is not required to register a member with the Club. The membership information collected by Clubs in relation to their members is jointly controlled by the GAA centrally and the GAA centrally should not have access to members' health information. If Clubs wish to collect medical information of members, due to medical information being classed as a 'special category' of personal data, the Club should be aware it requires a more stringent level of protection and should be stored securely and accesses only by those with a genuine requirement to access it.

6) Does GDPR prevent Clubs from publishing a list of paid members on notice board in the Club?

It is included within GAA Rule in the Official Guide that Clubs are required to publish a list of paid members on the notice board within the Club. As it included within GAA Rule, Clubs must comply with this. This is referred to within the Official Membership Forms when the member signs the form agreeing that their personal data will be used in the following way: "I understand that my Personal Data will also be used for administrative purposes to maintain my Membership including club and team administration". The publication of names of paid members is an element of Club administration.

7) Does the GAA have updated advice on Social Media?

There is a new Social Media Policy incorporating GDPR requirements currently being finalised which will be sent to Clubs. Clubs should ensure this Policy is adhered to in order to ensure compliance with the GDPR, and also with various other responsibilities such as child protection.

8) How long should ID documentation for Garda vetting be stored?

ID documentation collected in relation to the process of Garda Vetting members, for example photocopies of passports, utility bills etc. should be stored for the maximum period of one year. The Office of the Data Protection Commissioner has advised that this should be the retention period for all ID documentation related to Vetting procedures. In order to streamline the process, once a Club is satisfied that the Vetting has been completed, the ID documentation associated with the application should be deleted. / her should be returned to the Club or deleted.

FAQs

9) Is there a secure method of electronic storage available to Clubs?

Yes. The GAA OneDrive is a secure method of storing electronic information within Clubs. Access to OneDrive is available to anyone with an @gaa.ie email address. The username and password is the same as that used to sign into your @gaa.ie email. GAA related files should be stored (and shared, if necessary) using the GAA Office 365 system. This allows the club to retain control of the data (and ownership if someone changes role within the club) whilst ensuring that data is secure, backed up and available irrespective of hard disk issues (as can happen on Laptops or PCs). The Office 365 OneDrive is governed by a contract that ensures the GAA (the relevant club) has the right to recover / delete any information held therein. It also mandates that GAA data does not leave the EU.

10) Can Club volunteers use personal laptops/tablets/PC's to conduct Club related business?

Many clubs rely on their officers to use their own PCs to conduct GAA business. All of the GAA's systems are web based and, as a result, are accessible from any internet connected device. The data belonging to the Club should be stored within those systems (i.e. within the registration system or within OneDrive). Any spreadsheets or word documents that reside on the local drive should be password protected by clicking File in the top left corner and 'protect document'. One of the key requirements of GDPR is that a record or log of the locations of any personal data held by a club is recorded. This should include the fact that information is on the personal PC of the Secretary for example. If / when the Secretary changes role, the data that is held by him / her should be returned to the Club or deleted.

11) Can Clubs publish contact details of volunteers on the Club website?

Yes. Clubs can publish contact details of Club volunteers, for example, the groundsman on the Club website. However, the Club must ensure the individual in question has provided their consent for their information to be used in this manner. A sample consent form for this purpose is included within the GDPR Repository for Clubs.

12) Should Clubs implement a process around teamsheets?

Yes. An important element of games administration within the GAA is the provision of teamsheets to the referee and the opposing team prior to the match beginning. Clubs should ensure their teamsheets are stored in a secure manner together with the rest of the information Clubs hold, and that they are securely deleted on a regular basis. Teamsheets received from the opposition team should be treated with similar respect and deleted along with the Clubs own teamsheets once they are no longer required.