GUI Academy

GDPR Procedures

Last updated: 26th June 2018

Table of Contents

Our Procedures 3
Data protection laws 3
Who is responsible for data protection? 3
Implications of a breach 3
Key words in relation to data protection 4
Personal Data Explained: 4
Lawful basis for processing 4
Special Category Data 5
Data Protection Principles 6
Data Subject Rights 6
Notification and response procedure 7
Your main obligations 7
Your activities 7
Practical matters 8
Foreign transfers of personal data 9
Queries 9

Our Procedures

The Golfing Union of Ireland National Coaching Academy Limited is committed to complying with data protection legislation and to respecting the privacy rights of individuals. These procedures apply to all our directors, staff and volunteers **(Referred to as "Workers" throughout the document).**

These procedures set out our approach to data protection legislations and the principles that we will apply to our processing of personal data. The aim of these procedures is to ensure that we process personal data in accordance with the legislation and with the utmost care and respect.

These procedures apply to the Golfing Union of Ireland National Coaching Academy Limited. References in these procedures to "us", "we" and "our" are in relation to the three organisations. References to *"you"*, *"yourself"* and *"your"* are each worker whom these procedures apply.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with these procedures and to apply and implement their requirements when processing any personal data. ***Please pay special attention to sections pages seven, eight and nine as these set out the practical day to day actions that you must adhere to when working or volunteering for the organisation.***

The data protection legislation is a complex area. These procedures have been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. These procedures also set out the consequences of failing to comply with these legal requirements. However, these procedures are not an exhaustive statement of data protection legislations nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on these procedures, your responsibilities or any aspect of data protection law, seek advice from your line manager or the individual in your organisation that is responsible for data protection compliance.

Data protection laws

The General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 ("**DPA 2018**") (together "**Data Protection Laws**")

The Data Protection Laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

Who is responsible for data protection?

All our "Workers" are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

We are not required to appoint a Data Protection Officer (DPO). However, we have still appointed at least one person from each of the three organisations to be responsible for overseeing our compliance with data protection legislation.

Implications of a breach

- Any breaches of these procedures will be viewed very seriously. All Workers must read these procedures carefully and make sure they are familiar with them. Breaching of these procedures is a disciplinary matter and will be dealt with under each organisations Disciplinary Procedures.

There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:

For the worker:

- **Disciplinary action:** If you are an employee, your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. Where you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us.

- **Investigations and interviews**: Your actions could be investigated, and you could be interviewed in relation to any non-compliance.

Key words in relation to data protection

- **Personal data** is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, customer, prospective customer, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV). **Explained further in section four**.
- **Identifiable** means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. if a name or video footage) or might do if taken together with other information available to or obtainable us (e.g. a job title and organisations name).
- **Data subject** is the living individual to whom the relevant personal data relates.
- **Processing** is widely defined under data protection law and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.
- **Data controller** is the person who is responsible for controlling how personal data is used
- **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller and in accordance with the privacy policy.

Personal Data Explained:

Data will relate to an individual and therefore be their personal data if it:

- Identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
- Its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;
- It could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post);
- Information about companies or other legal persons is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often personal data, so business related information can often be personal data.
- Examples of information likely to constitute personal data:
    - Unique names;
    - Names together with email addresses or other contact details;
    - Job title and employer (if there is only one person in the position);
    - Video - and photographic images;
    - Information about individuals obtained as a result of Safeguarding checks;
    - Medical and disability information;
    - CCTV images;
    - Member profile information (e.g. marketing preferences); and
    - Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

Lawful basis for processing

For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

For the processing of ordinary personal data in our organisation these may include, among other things:

- the data subject has given their consent to the processing (perhaps giving when they join the organisation as a volunteer/staff member and complete a contact form)
- the processing is necessary for the performance of a contract with the data subject (for example, for processing tournament entries);
- the processing is necessary for compliance with a legal obligation to which the data controller is subject (such as reporting employee PAYE deductions to the tax authorities); or

- the processing is necessary for the legitimate interest reasons of the data controller or a third party (for example, keeping in touch with members, players, participants about competition dates, upcoming fixtures/workshops/events).

Special Category Data

Special category data under the Data Protection Laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, biometric data and genetic data.

Under Data Protection Legislation this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

- the processing is necessary for the performance of our obligations under employment law;
- the processing is necessary to protect the vital interests of the data subject;
- the processing relates to information manifestly made public by the data subject;
- the processing is necessary for the purpose of establishing, exercising or defending legal claims; or
- the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.
- To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:
    - ensure that either the individual has given their explicit consent to the processing; or
    - ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

We would normally only expect to process special category personal data or criminal records history data usually in a Human Resources context and in the context of our volunteers for safeguarding checks, health and safety etc

When do we process personal data?

Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

Examples of processing personal data might include:

- Using personal data to correspond with golf club officials/members;
- Holding personal data in our databases or documents; and
- Recording personal data in personnel or member files.

Outline

The main themes of the Data Protection Legislations are:

a. good practices for handling personal data;
b. rights for individuals in respect of personal data that data controllers hold on them; and
c. being able to demonstrate compliance with these laws.

In summary, data protection law requires each data controller to:

- only process personal data for certain purposes;
- process personal data in accordance with the six principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);
- provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice, for example you will have received one of these from us as one of our Workers;
- respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and
- keep adequate records of how data is processed and, where necessary, notify the Data Commissioner and possibly data subjects where there has been a data breach.

Every Worker has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with these procedures.

Data protection law in the ROI is enforced by the Data Commissioner's Office and in NI it is enforced by Information Commissioners Office.

Data Protection Principles

The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

1. processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
2. collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");
3. adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");
4. accurate and where necessary kept up to date;
5. kept for no longer than is necessary for the purpose ("storage limitation");
6. processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

Data Subject Rights

Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary, these are:

- The rights to access their personal data, usually referred to as a subject access request
- The right to have their personal data rectified;
- The right to have their personal data erased, usually referred to as the right to be forgotten;
- The right to restrict processing of their personal data;
- The right to object to restrict processing for example direct marketing materials;
- The right to portability of their personal data;
- The right to not be subject to a decision made solely by automated data processing (profiling).

The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by us (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request.

Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However, the right to not receive marketing material is an absolute right, so this should be complied with immediately.

Where an individual considers that we have not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the Data Protection Commissioners or Information Commissioners Office.

In addition to the rights discussed in this document, any person may ask the Data Protection Commissioners or Information Commissioners Office to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The Data Protection Commissioners or Information Commissioners Office must investigate and may serve an "Information Notice" on us (if we are the relevant data controller). The result of the investigation may lead to an "Enforcement Notice" being issued by the Data Protection Commissioners or Information Commissioners Office.

In the event of a Worker receiving such a notice, they must immediately pass the communication to the person responsible for GDPR in your organisation.

Notification and response procedure

If a Worker has a request or believes they have a request for the exercise of a Right, they should:

- pass the call to their line manager or person responsible for GDPR in their organisation. From here the person responsible should take and record all relevant details and explain the procedure. If possible, try to get the request confirmed in writing addressed to the person responsible for GDPR in your organisation
- inform the person responsible for GDPR in your organisation of the request.

If a letter or fax exercising a Right is received by any Worker, they should:

- pass the letter to their line manager or person responsible for GDPR in their organisation.
- the line manager or person responsible for GDPR must log the receipt of the letter with the person responsible for GDPR in your organisation and send a copy of it to them;
- the person responsible for GDPR in your organisation will then respond to the data subject on our behalf.

If an email exercising a Rights is received by any Worker, they should:

- pass the email to their line manager/person responsible for GDPR in their organisation
- the line manager/person responsible for GDPR in their organisation must log the receipt of the email with the person responsible for GDPR in your organisation and send a copy of it to them; and
- the person responsible for GDPR in your organisation will then respond to the data subject on our behalf.

The person responsible for GDPR in your organisation will co-ordinate the appropriate response which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request. The person responsible for GDPR in your organisation will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the person responsible for GDPR in your organisation should suffice in most cases.

The person responsible for GDPR in your organisation will inform the relevant management line of any action that must be taken to legally comply. The person responsible for GDPR in your organisation will co-ordinate any additional activity required by the IT providers to meet the request.

The manager/senior manager who receives the request will be responsible for ensuring that the relevant response is made within the time period required.

The person responsible for GDPR in your organisation's reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by legal advisors.

Your main obligations

What this all means for you can be summarised as follows:

- Treat all personal data with respect;
- Treat all personal data how you would want your own personal data to be treated;
- Immediately notify your line manager or the person responsible for GDPR in your organisation if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;
- Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and
- Immediately notify the person responsible for GDPR in your organisation if you become aware of or suspect the loss of any personal data or any item containing personal data.

Your activities

Data protection laws have different implications in different areas of our organisation and for different types of activity, and sometimes these effects can be unexpected.

Areas and activities particularly affected by data protection law include human resources, payroll, security (e.g. CCTV), customer care, sales, marketing and promotions, health and safety and finance.

You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply always with these procedures.

Practical matters

Whilst you should always apply a common-sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of Dos and Don'ts under the relevant headings:

Training

- Always ensure that all directors, staff and volunteers are educated on their responsibility in relation to GDPR.

PC's/Laptops/Printers/Mobile Phones:

- Only disclose your unique logins and passwords for any of our IT systems to authorised personnel and not to anyone else.
- Always lock PC's, laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use
- When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.

Using Data

- When in public place, e.g. a train or clubhouse, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary, move location or change to a different task.
- Ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.
- Do not transfer personal data to any third party without prior written consent of your line manager or person overseeing GDPR in your organisation.
- When sending out large group emails, ensure that you use the Blind Carbon Copy (BCC) feature to protect the privacy of email addresses
- Always ensure that people have the option to unsubscribe to newsletters/marketing material/updates

Storing Data

- Do not leave personal data lying around, store it securely.
- Password protect documents and databases containing personal data
- Never leave any items containing personal data unattended in a public place, e.g. on a train, in the bar of a clubhouse, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.
- Never use removable storage media to store personal data unless the personal data on the media is encrypted (password protected)

Disposing of Data

- Dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
- Use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

Loss of Data

- If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our person overseeing GDPR in your organisation.

WiFi

- When accessing WiFi to process data it must be an encrypted WiFi (password protected)

Championships/Workshops/Seminars

- All application/registration forms should include relevant "opt in" functions

- Data may be stored and processed for the purpose of the "***event"***
- Unless permission has been granted, following the "***event"*** data should be disposed of in the appropriate manner (e.g deleted from PC's, Laptops, shredded etc)
- All U-18s must have **signed** parental consent for the processing of data

Panels & Teams

- All contact forms should include relevant "opt in" functions
- Data may be stored and processed for the length of time the individual is on a panel/team or acting as a team manager/captain to that team
- Unless permission has been granted, once the individual is no longer a member of the panel/team data should be disposed of in the appropriate manner (e.g deleted from PC's, Laptops, shredded etc)
- All U-18s must have **signed** parental consent for the processing of data

Always notify your line manager or person overseeing GDPR in your organisation immediately of any suspected security breaches or loss of personal data.

However, you should always take a common-sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of your line manager or the person responsible for GDPR in your organisation.

Foreign transfers of personal data

Personal data must not be transferred outside the European Economic Area (**EEA**) unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections. This is mainly relevant to data held and accessed in Cloud-based services as well as some data processing the club may outsource like payroll processing or performance data analysis

These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or due to the fact that the recipient's own country's laws provide sufficient protection.

These restrictions also apply to transfers of personal data outside of the EEA even if the personal data is not being transferred outside of our group of companies.

- You must not under any circumstances transfer any personal data outside of the EEA without your line manager's or the person responsible for GDPR in your organisation prior written consent.
- We will also need to inform data subjects (e.g. players/team captains/coaches) of any transfer of their personal data outside of ROI/NI and may need to amend their privacy notice to take account of the transfer of data outside of the EEA.
- If you are involved in any new processing of personal data which may involve transfer of personal data outside of the EEA, then please seek approval of your line manager prior to implementing any processing of personal data which may have this effect.

Queries

If you have any queries about these procedures, please contact either your line manager or the person responsible for GDPR in your organisation.