V1| JANUARY 2022

ENGLAND ATHLETICS CLUB GUIDE

GDPR

ENGLAND ATHLETICS

GDPR

CONTENTS

Welcome to our GDPR Guide

This guide is intended for use by the club committee. Club committee members are responsible for supplying and maintaining guidance to volunteers within their relevant club for data capture, transfer, storage, and retention.

01. GUIDE TO GDPR

WHAT IS THE GDPR, OR GENERAL DATA PROTECTION REGULATION?

Definition: **A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).**

What is the goal of GDPR: To raise the standards for processing personal data, to strengthen and unify protection for individuals across the EU.

Twenty years ago the world was a very different place. The reach of technology was limited, and the way organisations used and processed your personal data was very different to how they use it today. The changes that have happened over the last two decades have forced the European Union (EU) to review the old legislation and bring them up to speed with the modern era.

The new legislation came into force in the UK on 25th May 2018 and will exist post-Brexit.

Aim of this Guide

This guide is an educational tool and acts as a guide to the GDPR and how it may affect your club's processes.

It includes guidance on:
1. The assessment of the data you control
2. The on-going risk management of this data
3. The reactive response processes that should be followed.

It has been created in partnership with Black Penny Consulting.

GLOSSARY OF TERMS

Personally Identifiable information (PII) or Personal Data

Any information that can be used to identify an individual. Examples could be names, addresses, telephone numbers right through to more sensitive types of information such as religion, ethnicity and disabilities.

Data Subject

This is an individual. For the clubs this could be athletes, coaches or parents and guardians.

Data Controller

This is the owner and user of the gathered personal data. This is anybody gathering and retaining personal data, such as the club committee.

Data Processor

This is a company, organisation or individual who processes the data on behalf of the data controller. This could be a membership management database.

Lawful Processing

The legitimate reason for holding and processing personal data, such as being necessary for performance of a contract with the athletes.

Subject Access Request (SAR)

This is a request from an individual to the club to find out what information you hold on them. They also have the right to request that you change or permanently remove any details that you hold on them.

Breach

This is the loss of information. This could come from a hacker or physically losing files/folders.

Data Protection Officer (DPO)

Representative for data protection duties.

02. HOW TO ASSESS YOUR DATA

ASSESSING YOUR DATA USING THE GDPR FRAMEWORK REGISTER

The GDPR Framework Register acts as an initial Privacy Impact Assessment (PIA) and a register of alignment process.

It will also hold the detail that has been gathered on personal data use within the club.

1 Watch the video guides on the England Athletics ClubHub.

This series of videos will guide you through completion of the GDPR Framework Register.

You can download the GDPR Framework Register on the England Athletics Club Hub.

2 Complete the GDPR Framework Register.

The Excel document helps work out if your club needs to make any changes in order to align with the GDPR.

Use the document tabs in number sequence and follow the guidance notes in the yellow boxes.

This detail will need to be kept up to date as part of future changes and impact assessments.

INSTRUCTIONS FOR COMPLETING THE GDPR FRAMEWORK REGISTER

You can download the GDPR Framework Register on the England Athletics Club Hub.

1. Open the GDPR Framework Register.

2. If the 'Enable Content' button is displayed in the top bar, press it.

3. Open the 'GDPR Alignment Checklist' tab:

a) This tab is to be used to capture progress of assigning tasks and completing them.

b) Review the tasks used to measure GDPR alignment.

c) Assign tasks as required. When assigned enter the number '1' against the task in the 'Assigned' column.

d) When the task has been completed, enter the number '1' against the task in the 'Completed' column.

4. Open the 'Athletes - Parents' tab, answer the following about the collection of personal data on the athletes and parents within local athletics. Where there isn't a matching answer, make sure 'Other…' is visible and add this detail in the 'Data Inventory' tab.

a) Review the methods of personal data collection and deselect all that do not apply.

b) Review the methods of personal data storage and deselect all that do not apply.

c) Review the ways the personal data can be passed on and deselect all that do not apply.

d) Review the recipients of personal data pass on and deselect all that do not apply.

5. Open the 'Coach – Committee Members' tab, answer the following about the collection of personal data on the coach and committee members within your club. Where there isn't a matching answer, make sure 'Other…' is visible and add this detail in the 'Data Inventory' tab.

a) Review the methods of personal data collection and deselect all that do not apply.

b) Review the methods of personal data storage and deselect all that do not apply.

c) Review the ways the personal data can be passed on and deselect all that do not apply.

d) Review the recipients of personal data pass-on and deselect all that do not apply.

You can download the GDPR Framework Register on the England Athletics Club Hub.

6. Open the 'Data Inventory' tab. This sheet is designed to capture further detail on the personal data that is captured and processed as part of club activities. The sheet has been pre-populated with details that should already be applicable. If a process you use is not listed in the 'Process' column, add it to the bottom of the list:

a) Review the process in the 'Process' column. If this does not apply to you then simply edit the 'Comments' column and enter 'Not in use'.

b) If incorrect, edit the direction of the process from the column labelled 'Direction'. Inbound means data coming into the club.

c) If incorrect, edit the owner of the process from the column labelled 'Owner'. This is the person who carries out the data gathering process.

d) If incorrect, edit the description of the process from the column labelled 'Description'. Give as much detail as possible on the activity in the process.

e) If incorrect, select the type of data in the process from the column labelled 'What'. Personal data is classed as sensitive when it includes: religion, ethnicity, health care records etc.

f) Select all the personnel who can access the data in this process. If there are others not on the list, add these to the 'Comments' column.

g) Select all the methods by which the data is received and transferred in this process. If there are others not on the list, add these to the 'Comments' column. Use the detail from the '… Journey' tabs as assistance.

h) Select all the locations where the data in this process is stored. If there are others not on the list, add these to the 'Comments' column.

i) If incorrect, edit the purpose for the process from the column labelled 'Why'. Give further detail to justify the data collection.

j) If incorrect, edit the detail for how long the data is retained for the process from the column labelled 'When'. Give further detail on the reasons for retaining the data.

k) The 'Comments' column should be used as instructed above and for any further detail you feel is required to justify the data gathering process.

You can download the GDPR Framework Register on the England Athletics Club Hub.

7. Open the 'Data Security' tab. This sheet is designed to capture the data security in place for the various means of handling personal data within your club. The sheet has been pre-populated with details that should already be applicable. If a media you use is not listed in the 'Data Process Media' column, add it to the bottom of the list.

a) Review the Media in the 'Data Process Media' column, if this does not apply to you then edit the 'Description' column and enter 'Not in use'.

b) If incorrect, edit the storage of the media from the column labelled 'Data Storage'. Data storage is where data is stored, such as a filing cabinet.

c) If incorrect, edit the security of the media from the column labelled 'Security'. Security is the mechanism used to keep the data media safe.

d) If incorrect, edit the name of the vendors of the media from the column labelled 'Vendor'. This will be the vendor of the technology used for the media process.

e) If incorrect, edit the description of the process media from the column labelled 'Description'. Add detail to demonstrate the security in place to protect the personal data.

f) If incorrect, edit the risk of the process media from the column labelled 'Risks'. This column is used to capture highlighted risks, these should also be present in the 'Risk Register' tab.

8. Open the 'Lawful Processing Records' tab. This sheet is designed to capture the justified means by which you are capturing, using, and transferring personal data within the club. The sheet has been pre-populated with details that should already be applicable. This sheet has been partially populated from the input completed in the 'Data Inventory' tab. If a process has not appeared as expected, add it to the bottom of this sheet.

a) Review the following pre-populated columns: 'System…', 'The name…', 'The purposes…', 'A description of…', 'Where possible….

b) If incorrect, edit the data that is captured as part of the process in the column for examples of data captured. This information determines whether it is classified as sensitive or not.

c) If incorrect, select justification code for the process in the column labelled 'Lawful Process Article'. This refers to the legal and general description of the code that can be found in the table to the right of the sheet.

d) Enter the name of the approving committee member for this process being lawfully justified. This should also include a date of the approval.

You can download the GDPR Framework Register on the England Athletics Club Hub.

9. Open the 'Third Party Processors' tab. This sheet is designed to capture the third-party processors that have access to the personal data within your club. These will typically be providers of technology services such as membership management software or even online cloud storage repositories. The sheet has been pre-populated with details that should already be applicable. If a third-party processor you use is not listed in the 'Third Party' column, add it to the bottom of the list.

a) Review the name in the 'Third Party' column, if this does not apply to you then simply edit the 'Detail' column and enter 'Not in use'.

b) If incorrect, edit the name of the service offered by the third party from the column labelled 'Service'.

c) If incorrect, edit the detail of the third-party service offered from the column labelled 'Detail'. Add further detail on the provider.

d) Enter the period the data will be kept for in the column labelled 'Retention Period'. If a period is not defined type 'Undefined' and add this as a risk to the 'Risk Register' tab.

e) Enter the date the contract is due for renewal in the column labelled 'Contract Renewal Date'. If this is unknown, type 'Unknown'.

f) Enter 'Yes' in the column labelled 'Incident Reporting Process' if one exists between yourselves and the third-party processor. If this does not exist, then type 'Undefined' and add this as a risk to the 'Risk Register' tab.

g) Enter 'Yes' in the column labelled 'GDPR Complaint' if the third-party processor has confirmed their GDPR alignment. If this has not happened yet, then type 'Unconfirmed' and add this as a risk to the 'Risk Register' tab.

You can download the GDPR Framework Register on the England Athletics Club Hub.

10. Open the 'Risk Register' tab. This sheet captures the active risks associated to the personal data within your club and how specifically it is gathered, stored, and transferred. The sheet has been pre-populated with details that should already be applicable. If a risk you identify is not listed in the 'Risk' column, add it to the bottom of the list.

a) Review the detail in the 'Risk' column, if this does not apply to you then simply edit the 'Recommendation' column and enter 'Not Applicable'.

b) If incorrect, edit the functional owner of the risk from the column labelled 'Functional Area'. This is the overarching responsible party.

c) If incorrect, edit the operational owner of the risk from the column labelled 'Owner'. This will be the functional risk owner.

d) If incorrect, edit the detail of the risk from the column labelled 'Risk'. Add further detail.

e) If incorrect, select the risk severity from the column labelled 'Priority'. This highlights the impact of the risk.

f) If incorrect, enter an amount estimated as the commercial exposure of mitigating the risk from the column labelled 'Cost'. This is to highlight potential cost exposure of mitigation.

g) If incorrect, change the status of the risk as it stands currently from the column labelled 'Status'. This is to highlight the risks outstanding.

h) Add detail of the mitigation being reviewed for the risk in the column labelled 'Mitigation'. This should include as much detail as possible to demonstrate positive steps are being taken to mitigate or accept the risks.

You can download the GDPR Framework Register on the England Athletics Club Hub.

11. Open the 'Privacy Notice Register' tab. This sheet is designed to capture the existence of privacy notices for the gathering of personal data within your club. The sheet has been pre-populated with details that should already be applicable. If a privacy notice you identify is not listed in the 'Name' column, add it to the bottom of the list.

a) Review the detail in the 'Name' column. If this does not apply to you then simply edit the 'Notes' column and enter 'Not Applicable'.

b) If incorrect, edit the name of the privacy notice from the column labelled 'Name'. This is the name of the privacy notice in place, or the privacy notice that is required.

c) Edit the date of the privacy notice issue date in the column labelled 'Privacy Notice'. This can have already passed or the date the new privacy notice will go live.

d) If incorrect, edit the location of the privacy notice from the column labelled 'Location'. Add detail.

e) If incorrect, edit the detail of the privacy notice from the column labelled 'Notes'. Add detail.

f) If incorrect, select the status of the privacy notice from the column labelled 'GDPR Ready'. This needs to indicate if the privacy notice adheres to the guidance by the Information Commissioner's Office (ICO).

03. MANAGING DATA RISKS

MANAGING THIRD PARTY PROCESSES

An obligation when aligning to the GDPR is that all third-party processors you identify have been assessed for their alignment to the GDPR.

This assessment requires them to be issued with a checklist of obligations and their response to be logged.

If a third-party processor does not acknowledge the checklist or can't align to the controls within it, you as the responsible club committee need to decide if you wish to seek an alternate provider or accept, justify, and document the risk in the Risk Register within the GDPR Framework Register.

N.B. Many large service providers, such as Microsoft and Google, have statements on their websites that address the controls in the checklist. **These providers will not need to be approached** and this should be checked in advance of sending them the checklist.

The checklist can be found on the following page and should be sent to all identified parties that do not have statements on their websites, as part of the GDPR Framework Register completion.

CHECKLIST

Requirement	Yes/No	Comment
Please confirm that you are GDPR Compliant (Detail relevant Technical & Organisational security measures).		
Can we search for our personal data on your systems?		
Can we delete our personal data from your systems?		
Can we export our personal data from your systems?		
Do your standard contract terms include the new GDPR mandatory provisions?		
Are you maintaining Data Processing Records?		
Do you have a documented Breach Notification Process?		
Can you confirm your ability to have our personal data deleted or upon termination of contract at no extra cost?		
Can you confirm you offer full transparency of data transfer to other parties/destinations?		
Can you confirm you have a documented Sub-processor change request process?		

BREACH NOTIFICATIONS

The club committee has an obligation to assess, report and notify (if applicable) any breaches within your club.

The 'Breach Notification Process' outlines:

1. Identification and assessment
2. Containment and recovery
3. Risk assessment
4. Notification
5. Evaluation and response.

This process should be followed for all reported cases of a breach.

A breach can be defined as:

- The disclosure of confidential data to unauthorised individuals
- The loss or theft of portable devices or equipment containing identifiable personal, confidential, or sensitive data, PCs, USBs, mobile phones; laptops, disks etc
- The loss or theft of paper records
- Inappropriate access controls allowing unauthorised use of information
- A suspected breach of IT security
- Attempts to gain unauthorised access to computer systems, for example hacking
- Records altered or deleted without authorisation from the data 'owner'
- Viruses or other security attacks on IT equipment systems or networks
- Breaches of physical security for example forcing of doors or windows into a secure room or forcing open a filing cabinet containing confidential information
- Confidential information left unlocked in accessible areas
- Insecure disposal of confidential paper waste
- Leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information
- Publication of confidential data on the internet in error and accidental disclosure of passwords
- Mis-directed emails or faxes containing identifiable personal, confidential, or sensitive data.

A suspected or actual breach will likely be detected by a volunteer within a group. When such a situation happens, the member should be given a copy of the Breach Notification Form.

If they detect an actual breach, they must complete the form and pass it to the club committee as quickly as possible for further analysis and response as above.

Remember: If a breach is assessed to be a certain severity, then the ICO need to be made aware within 72 hours of first discovering it. Further details can be found on the ICO website.

Subject Access Request (SAR) Process

An obligation you have as the club committee is to assess, complete and notify data subjects after a SAR.

Please see Section 04 of this guide for a step-by-step guide to managing a SAR.

04. THE SUBJECT ACCESS REQUEST PROCESS (SAR)

THE SUBJECT ACCESS REQUEST PROCESS (SAR)

Any individual, or data subject, you hold data on is entitled to ask for that information through a process known as Subject Access Request (SAR).

The club committee is responsible for the application and effective working of this process, (but may need help from volunteers within the club from which the SAR has been requested).

Data subjects have the legal right to know whether you are processing any personal data about them and, if so, to be given:

- The purposes of you processing the data on them
- The categories of personal data concerned, personal or sensitive
- The recipients to whom the personal data has been or will be disclosed, particularly if in international organisations
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request from the controller rectification or erasure of personal data or restriction on processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a supervisory authority
- Any available information as to the source if you were not the originating data collector
- The existence of automated decision-making, including profiling. Detail needs to be available on what technologies are used here and what result this has on the data subject and their data.

The response to the data subject needs to be within one month, post-verifying their identity and the scope of the request. This can be extended by a further month, followed by one more month if the request cannot be completed in time - but notice must be given to the data subject on the extension and the reason why.

Discovery

Discovery will entail either:

- Collecting the data specified by the data subject, or
- Searching all databases and all relevant filing systems (manual files) in the club, including all readily available back up and archived files.

It is suggested that the club committee maintain a data map that identifies where all club data is stored to make it easier and quicker when undertaking searches.

PROCEDURE

It is suggested that club committees follow this procedure and use the forms detailed within the steps when processing Subject Access Requests:

1 Application

Data subject to provide request scope, or complete SAR Form. A copy of this can be found in the Club Hub.

2 Identity Evidence

The data subject must provide proof of identity in the form of a current passport/driving license (Signature to be cross-checked) or security questioning.

3 Request Logged

The date by which the identification checks, and the specification of the data sought must be recorded in the SAR Register in the GDPR Framework Register.

4 Discovery

The club committee discovers all instances where the data subject's personal data is present.

5 Response

The club committee responds to the data subject in electronic format and response logged.

RESPONDING TO A SAR

The club committee is responsible for reviewing all provided documents to check whether any third parties are identified in it and for either omitting or redacting identifying third party information from the documentation, or obtaining written consent from the third party for their identity to be revealed.

If the requested data falls under one of the following exemptions, it does not have to be provided:

- Crime prevention and detection
- Negotiations with the requester
- Information used for research, historical or statistical purposes
- Information covered by legal professional privilege.

The information will be provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

In all cases care should be taken to redact or censor all personal data or confidential information that the data subject should not see.

05. THE CLUB JOURNEY

STAGES OF THE CLUB JOURNEY

This table details the stages of the club journey when England Athletics collects and processes personal data on athletes, their parents, club committee members and coaches.

It also includes a brief outline of its significance in terms of GDPR.

STAGE	What does this mean for GDPR?
Club committee member or coach joining New committee members and coaches pass their personal data to you via: • **E-mail** • **Face to Face** • **Registration Form.**	The gathering of information from a new committee member or coach is required for the **performance of the contract** between you and them but care needs to be taken to keep these communications private, especially when **personal data** is shared, such as in the Joiners Form, which may contain **sensitive data**.
New athletes joining form The new athletes joining form is used to capture information on the athlete to convert them to an active member, this could be via: • **E-mail** • **Web Form** • **Paper Form.**	The new athletes joining form will be the first data capture exercise for a new athlete. The form itself needs to consider and inform of data use: • **Purpose** – what are you going to do with it • **Limit** – it only includes what you need • **Retention** – delete when no longer required • **Secure** – special care taken in storing • **Transfer** – who receives this data.

STAGE	What does this mean for GDPR?
Active member The athlete and parent/guardian are now active within the club.	The athlete data will probably be stored in a main filing system such as a membership database, Excel sheets on local laptops and/or paper-based records. During this period you need to consider: • **Third party processors** – holding data on your behalf, such as membership databases • **Accuracy** – keep data up to date • **Data privacy** – how secure is the data.
Fundraising The club requires funding to offer the services for athletes and parents, specifically for equipment and event funding.	The new funders joining form will be the first data capture exercise for a new donor. The form itself needs to consider and inform of data use: • **Purpose** – what are you going to do with it • **Limit** – it only includes what you need • **Retention** – delete when no longer required • **Secure** – special care taken in storing • **Transfer** – who receives this data.

STAGE	What does this mean for GDPR?
Events and competitions Events and competitions are held frequently for the athletes. These can be: • **Race meetings** • **Social events.** These events can require further data gathering, such as Guardian Consent and Health forms.	When further data gathering is being completed you need to consider: • **Purpose** – what are you going to do with it • **Limit** – it only includes what you need • **Retention** – delete when no longer required • **Secure** – special care taken in storing. This activity should consider what data you already have on file and only capture what is necessary.
Club surveys Athletes' data may be presented to the club committee to allow for statistical analysis. This may include: • **Religion** • **Ethnicity.**	Transfer of personal data of any kind needs to be handled with due care, especially with details considered **sensitive**, such as ethnicity and religion. In all cases the purpose of the transfer should be well understood and documented with techniques such as **anonymising** the data being used.

STAGE	What does this mean for GDPR?
Register At every training session and competition the coach has an obligation to take a register of the athletes attending the session.	Registration of athletes for each meeting is good practice from a safeguarding perspective. What this does highlight though is the importance of the following: • Accurate data on the athletes • Maintaining a log of attendees but retaining strong data protection, such as use of digital data as opposed to paper records and a minimised data set purely for attendance.
Comms Part of being a club committee in athletics is the requirement to keep the athletes and parents updated. These updates are for weekly training, upcoming events/ competitions and general club news.	Communication to the athletes and parents is essential for the fluent operation of the club. The GDPR recognises these types of communications and categorises them as necessary for fulfilling your role. However, this communication should only be for the purposes of the club and not for further advertising, unless they have specifically opted-in.

STAGE	What does this mean for GDPR?
Waiting Lists When the club reaches capacity the coach or club committee maintain a list of athletes and their parents to keep in contact when space becomes available. This communication could be via e-mail or telephone conversation.	When data is being held due care needs to be taken in the storage. In addition, the information being held needs to be **accurate** and **minimised**. If at any time the athlete or parent wishes to leave the waiting list their data should be deleted fully if not required for further purposes. All personal data should have a defined and appropriate retention period for its storing.
Breach It may occur that personal data is disclosed externally accidently or removed from the club via malicious means. Athletes and parents may also exercise rights they have over their data you hold.	In the event of a **breach**, via malicious means or through accidental disclosure, the **data controller** is obligated to do the following: • Report the **breach** to the **DPO** • Complete a **Breach Response Form.** In the event an athlete or parent requests their data to be **deleted**, **updated** or **disclosed,** the data controller has one month to complete the request if not deemed excessive.

STAGE

What does this mean for GDPR?

Leavers

From time-to-time athletes, coaches and committee members leave the club. This means that their association with the club ceases and as part of this the club sets the data held on the individuals as archived.

When the individual wishes to leave the club, the data held on them needs to be archived and consideration needs to be given to:

- **Limit** – it only includes what you need
- **Retention** – delete when no longer required
- **Secure** – special care taken in storing
- **Transfer** – who receives this data.

ENGLAND ATHLETICS

For more digital club support visit Club Hub