BLACK PENNY CONSULTING

ENGLAND ATHLETICS

The GDPR

How to guide for Club Officials

Version 1.0 - May 2018

Contents

Document Purpose

This document forms part of the GDPR guidance from England Athletics which has been created in partnership with Black Penny Consulting.

The audience for this document is the Club Officials of the club. The Club Officials who will complete this task must have a good working knowledge of the club and be in possession of the facts when it comes to data movements through the club. The guides and processes should be distributed to the volunteers for general consumption and, where possible, they should acknowledge receipt.

The GDPR guidance has been developed as an education tool and as a means to gather information for alignment to the GDPR.

The GDPR Framework Register acts as an initial Privacy Impact Assessment (PIA) and a register of alignment progress. The GDPR Framework Register will hold the detail that has been gathered on Personal Data use within the club. This detail will need to be kept up to date as part of future changes and Impact Assessments.

The Club Official is responsible for supplying and maintaining guidance to volunteers within their relevant club for data capture, transfer, storage and retention.

What's included

There are a number of documents included with the guidance. These are designed for the assessment of the data you control, the ongoing risk management of this data and the reactive response processes that should be followed.

Step 1 - How to assess your data

a) Read 'What is the GDPR'
b) Watch video guides
c) Complete the GDPR Framework

The following is a guide to help you complete an initial Privacy Impact Assessment (PIA).

A Privacy Impact Assessment, also known as a Data Privacy Impact Assessment is the assessment conducted when a change happens that could affect the data privacy of the club and change the baseline captured as part of the initial PIA.

The idea behind a PIA is to run the change through the GDPR Framework Register and measure its risk. This is an ongoing obligation of the Club Officials.

a) What is GDPR?

This is initial guidance on what GDPR is and some examples of its impact on day-to-day Athletics.

1. Open 'What is GDPR'.
2. Read the document.

b) Video guides

This is a series of videos that will guide you through completion of the GDPR Framework Register

1. Watch the GDPR framework register video guides at vimeopro.com/englandathletics/data-protection

c) The GDPR Framework Register

This is an Excel spreadsheet to help you work out if any changes are needed to make your club aligned with the GDPR. Use the document tabs in number sequence and follow the guidance notes in the yellow boxes.

1. Open 'GDPR Framework Register.xlsm'.
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 with regards to 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 – Club Officials’ tab, answer the following with regards to the collection of personal data on the Coach and Club Officials within your club. Where there isn’t a matching answer, make sure ‘Other…’ is visible and add this detail is captured 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
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 as much detail as possible on the reasons 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 as much detail as possible on the reasons for retaining the data as long as described.
k. The ‘Comments’ column should be used as instructed above and for any further detail you feel is required to give justification to the data gathering process.

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 simply 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 and private.
   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 as much detail as possible to demonstrate the security in place to protect the security and privacy of 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 helps determine 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 Club Official of your club for this process being lawfully justified. This should also include a date of the approval.

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 as much detail as possible 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' in the column.

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.

10. Open the ‘Risk Register’ tab. This sheet is designed to capture 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 is the functional risk owner.

d. If incorrect, edit the detail of the risk from the column labelled ‘Risk’. Add as much detail as possible.

e. If incorrect, select the risk severity from the column labelled ‘Priority’. This is to highlight 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.

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 potentially the privacy notice that is required.

c. Edit the date of the privacy notice issue date 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 as much detail as possible.
e. If incorrect, edit the detail of the privacy notice from the column labelled ‘Notes’. Add as much detail as possible.
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).

Step 2 – How to manage your data risks?

a) Contact third party processors
b) Distribute local response plan

The following is a guide to managing data risks through managing the third parties used and delivering local response plans for use in the event of data breach or Subject Access Request (SAR), also known as a Data Subject Access Request (DSAR).

a) Contact third party processors

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.

In the event that a third party processor does not acknowledge the checklist or can't align to the controls within it, you as the responsible Club Officials need to decide if you seek an alternative provider or accept, justify and document the risk in the Risk Register within the GDPR Framework Register.

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. Examples are:

Google - https://www.google.com/cloud/security/gdpr/

Microsoft - https://docs.microsoft.com/en-us/office365/enterprise/office-365-info-protection-for-gdpr-overview

This should be checked in advance of sending them the checklist.

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

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?		

b) Incident Response Plans

Breach Notification

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

The 'Breach Notification Process' is included in the GDPR guidance from England Athletics and designed as a step-by-step guide for managing a breach. It 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
- misdirected 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 from the GDPR Guidance. If they detect an actual breach, they must complete the form and pass it to the Club Official 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 Process

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

The ‘Subject Access Request Process’ is included in the GDPR Guidance and designed as a step-by-step guide for managing a DSAR. It outlines:

1. DSAR application
2. ID evidence
3. Request logged
4. Data discovery
5. Response

This process should be followed for all requested DSARs.

How to respond if something happens

An on-going obligation on the Club Officials is that data breach incidents or SAR's are dealt with appropriately and in time.

Data breach management

Data breach management is an obligation on the Club Officials that is ongoing. In the event of a breach, follow the guidance above in this document.

Subject Access Request

Subject Access Requests are an obligation on the Club Officials that is ongoing. In the event of a SAR, follow the guidance in this document.