| **Method of collecting personal data** | **What personal data is collected** | **Data Subject(s)** | **When is this data collected** | **Volume of personal data** | **Why is this data collected?** | **Where is data stored?** | **Security measures already taken?** | **Retention period and when are any updates carried out** | **Data Controller? Joint Data Controller?**  **Data Processor?** | **Has a suitable Privacy Notice been issued?** | **Person responsible for handling data** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *State any methods that your club use to collect personal information* | *State what specific information is collected* | *State who this data is relating to* | *State when this data is collected* | *State the approximate number of individuals you collect this information from* | *State why you collect certain information AND your lawful reason for doing so*  *Please refer to data processing in the notes section below* | *State where you store this personal information and where it is transferred to (both within the club and to any third parties).*  *E.g. do you make personal information accessible for coaches? If so, where is it then stored?* | *State what you currently do to keep this data safe* | *State how long do you keep this data for and when any updates are done of this data to ensure its accurate* | *State which is applicable to your club against each of your methods of collecting information* | *State yes or no and describe how you do this* | *State who has responsibility for handling the data* |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

Step ONE - insert club name - data INVENTORY (2019)

ASSESSING THE INFORMATION YOU HOLD, WHERE IT IS AND WHO HANDLES IT.

**Notes**

1. \*For each type of data processing undertaken, there must be a lawful basis for processing under Article 6 of the GDPR. The main lawful bases that the club may rely upon are:

* the processing is necessary to enter into or perform a **contract**;
* the processing is necessary to comply with a **legal obligation**;
* that the processing is necessary to pursue the **legitimate interests** of the club and does not cause unwarranted prejudice to the privacy rights of the individual;
* you have the **consent** of the individual (this should be relied upon sparingly because of the quality of consent required and the fact that Data Subjects must be free to withdraw their consent at any time, which can be problematic).

If your club wishes to process **special categories of personal data** you will need to have a lawful basis for doing so AND satisfy a specific condition from within Article 9 of the GDPR. Some examples of special categories of data are race, ethnic origin, politics, religion, health (which includes disability) and sexual orientation. The following link provides more information on special categories of data and Article 9 of the GDPR <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>.

1. \*\* **A Data Controller can be either individuals or "legal persons" such as companies, Government Departments, Clubs and voluntary organisations.**

For example; A data controller is responsible for the safe keeping and use of the Club members personal information on computer or in structured manual files. There are cases where the data controller is an individual include general practitioners, pharmacists, politicians and sole traders, where these individuals keep personal information about their patients, clients, constituents etc.

**A Joint Controller** is where two data controllers jointly own and share the same set of data and is usually backed up by a data sharing agreement.

For Example: If two Clubs organise a competition or event and jointly collect the data for the event and are keeping the data safe and are maintaining that data on a PC or in structured files. Then both are controllers of such data.

**A data processor** is any individual that processes personal data on behalf of the data controller.

For example; If a new member up loads their data to join a Club on line platform, then the online platform send that data to the Club, the online platform is a processor.

*Disclaimer*

This processing template is provided to you by the Athletics Northern Ireland for general information purposes only. The template is provided by Athletics Northern Ireland and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the inserted template contained herein. Any reliance you place on such information is therefore strictly at your own risk. Under no circumstances will the Athletics Northern Ireland be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or revenues arising out of, or in connection with, the use of this template. Clubs must therefore seek their own technical or legal advice on data protection matters, before implementing any measures within their setting

Step two - insert club name – GDPR Checklist (2019)

USE THE CHECK LIST BELOW TO ENSURE YOU HAVE COMPLETED EVERYTHING REQUIRED BY GDPR.

**Personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/ Remedial Action |
| Consent based data processing (Articles 7, 8 and 9 and further guidance available ) | Have you reviewed your Club’s mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of statement or a clear affirmative action? |  |  |  |
|  | If personal data that you currently hold on the basis of consent does not meet the required standard under the GDPR, have you re-sought the individual’s consent to ensure compliance with the GDPR? |  |  |  |
|  | Are procedures in place to demonstrate that an individual has consented to their data being processed? |  |  |  |
|  | Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data? |  |  |  |
| Children's personal data (Article 8) | Where online services are provided to a child, are procedures in place to verify age and get consent of a parent/ legal guardian, where required? |  |  |  |
| Legitimate interest-based data processing | If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? That analysis must demonstrate that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, and 3) the processing is not prejudicial to or overridden by the rights of the individual. |  |  |  |

**Data subject rights**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/ Remedial Action |
| Access to personal data (Article 15) | Is there a documented policy/procedure for handling Subject Access Requests (SARs)? |  |  |  |
|  | Is your organisation able to respond to SARs within one month? |  |  |  |
| Data portability (Article 20 and further guidance available | Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine-readable format? |  |  |  |
| Deletion and rectification (Articles 16 and 17) | Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)? |  |  |  |
| Right to restriction of processing (Article 18) | Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing? |  |  |  |
| Right to object to processing (Article 21) | Are individuals told about their right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest? |  |  |  |
|  | Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing? |  |  |  |
| Profiling and automated processing (Article 22 and further guidance available | If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected? |  |  |  |
|  | Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual’s right to obtain human intervention and to contest the decision? |  |  |  |
| Restrictions to data subject rights (Article 23) | Have the circumstances been documented in which an individual’s data protection rights may be lawfully restricted? Note: the Irish Data Protection Bill will set out further details on the implementation of Article 23. |  |  |  |

**Accuracy and retention**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/ Remedial Action |
| Purpose limitation | Is personal data only used for the purposes for which it was originally collected? |  |  |  |
| Data minimisation | Is the personal data collected limited to what is necessary for the purposes for which it is processed? |  |  |  |
| Accuracy | Are procedures in place to ensure personal data is kept up to date and accurate and where a correction is required, the necessary changes are made without delay? |  |  |  |
| Retention | Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected? |  |  |  |
| Other legal obligations governing retention | Is your business subject to other rules that require a minimum retention period (e.g. medical records/tax records)? |  |  |  |
|  | Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies? |  |  |  |
| Duplication of records | Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records? |  |  |  |

**Transparency requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/ Remedial Action |
| Transparency to customers and employees (Articles 12, 13 and 14 and further guidance available | Are service users/employees fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form using clear and plain language? |  |  |  |
|  | Where personal data is collected directly from the individuals, are procedures in place to provide the information listed at Article 13 of the GDPR? |  |  |  |
|  | If personal data is not collected from the subject but from a third party (e.g. acquired as part of a merger) are procedures in place to provide the information listed at Article 14 of the GDPR? |  |  |  |
|  | When engaging with individuals, such as when providing a service, sale of a good or CCTV monitoring, are procedures in place to proactively inform individuals of their GDPR rights? |  |  |  |
|  | Is information on how the organisation facilitates individuals exercising their GDPR rights published in an easily accessible and readable format? |  |  |  |

**Other data controller obligations**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/Remedial Action |
| Supplier Agreements (Articles 27 to 29) | Have agreements with suppliers and other third parties processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included? |  |  |  |
| Data Protection Officers (DPOs) (Articles 37 to 39 and further guidance available | Do you need to appoint a DPO as per Article 37 of the GDPR? |  |  |  |
|  | If it is decided that a DPO is not required, have you documented the reasons why? |  |  |  |
|  | Where a DPO is appointed, are escalation and reporting lines in place? Are these procedures documented? |  |  |  |
|  | Have you published the contact details of your DPO to facilitate your customers/ employees in making contact with them?  (Note: post 25 May 2018 you will also be required to notify your data protection authority of your DPO’s contact details) |  |  |  |
| Data Protection Impact Assessments (DPIAs) (Article 35 and further guidance available | If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented? |  |  |  |

**Data security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/ Remedial Action |
| Appropriate technical and organisational security measures (Article 32) | Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them? |  |  |  |
|  | Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data? |  |  |  |
|  | Is there a documented process for resolving security related complaints and issues? |  |  |  |
|  | Is there a designated individual who is responsible for preventing and investigating security breaches? |  |  |  |
|  | Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information? |  |  |  |
|  | Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained. |  |  |  |
|  | Can access to personal data be restored in a timely manner in the event of a physical or technical incident? |  |  |  |

**Data breaches**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Question | Yes | No | Comments/Remedial Action |
| Data Breach response obligations (Article 33 and 34 and further guidance available | Does the organisation have a documented privacy and security incident response plan? |  |  |  |
|  | Are plans and procedures regularly reviewed? |  |  |  |
|  | Are there procedures in place to notify the office of the Data Protection Commissioner of a data breach? |  |  |  |
|  | Are there procedures in place to notify data subjects of a data breach (where applicable)? |  |  |  |
|  | Are all data breaches fully documented? |  |  |  |
|  | Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches? |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **International data transfers (outside EEA) – *if applicable***   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | Question | Yes | No | Comments/Remedial Action | | International data transfers (Articles 44 to 50) | Is personal data transferred outside the EEA, e.g. to the US or other countries? |  |  |  | |  | Does this include any special categories of personal data? |  |  |  | |  | What is the purpose(s) of the transfer? |  |  |  | |  | Who is the transfer to? |  |  |  | |  | Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is?) |  |  |  | | Legality of international transfers | Is there a legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses. Are these bases documented? |  |  |  | | Transparency | Are data subjects fully informed about any intended international transfers of their personal data? |  |  |  | |

***Disclaimer***

This guide to data protection compliance is provided to you by the Athletics Northern Ireland for general information purposes only. The template is provided by Athletics Northern Ireland and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the inserted template contained herein. Any reliance you place on such information is therefore strictly at your own risk. Under no circumstances will the Athletics Northern Ireland be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or revenues arising out of, or in connection with, the use of this template. Clubs must therefore seek their own technical or legal advice on data protection matters, before implementing any measures within their setting