**Draft Data Protection Policy**

This is a Data Protection Policy template for a Club/League/Divisional Association. This template is not a legal document. Further information about data protection can be found by visiting the Information Commissioner Office (ICO) website.

1. **Introduction**
   1. The Club/League/Divisional Association is obligated and committed to comply with the General Data Protection Regulation 2018. This policy sets out our data protection responsibilities and how we deal with data protection matters internally.
   2. This policy is one of other Club/League/Divisional Association policies and a copy should be made available to all staff, volunteers, and others who process personal data for or on behalf of the Club/League/Divisional Association.
2. **Purpose**
   1. The Club/League/Divisional Association process personal data for purposes related to the game of football.
   2. This policy aims to ensure that our data processing is done without adversely affecting the rights of the individual.
   3. You must comply with this policy when processing personal data on behalf of the Club/League/Divisional Association, and this policy will help you to understand how to handle personal data to comply with the GDPR.
3. **Whose personal data we handle**
   1. The Club/League/Divisional Association process personal data about current, former, and prospective players.
   2. The Club/League/Divisional Association process personal data about parents/guardians if the player is a child.
   3. The Club/League/Divisional Association process personal data about employees, volunteers, members, referees, coaches, managers, contractors, third parties, suppliers, and other individuals that we communicate with (expand or add where necessary).
   4. The Club/League/Divisional Association process personal data about fans, supporters, and customers (expand or add where necessary)
4. **Data Protection Principles**
   1. Anyone processing personal data for, or on behalf, of the Club/League/Divisional Association must comply with the principles of the GDPR. The principles are:
      * Data is processed lawfully, fairly, and in a transparent manner
      * Data is processed with specific and explicit purpose
      * Data is limited to what is necessary for the purpose
      * Data is accurate and up to date
      * Data is kept no longer than is necessary
      * Data is protected using both technical and organisational measures
   2. The Club/League/Divisional Association is responsible for and must be able to demonstrate compliance with the data protection principles listed above.
5. **Lawful Processing**
   1. Lawful processing means data must be processed with a legal basis as set out in the GDPR.
   2. The following table sets out ways the Club/League/Divisional Association plan to use personal data, and the lawful basis to do so.

|  |  |
| --- | --- |
| **Activity** | **Lawful basis** |
| Processing player information including payment | Performance of a contract |
| Organising matches and events | Performance of a contract |
| Communicating club information and updates | Performance of a contract |
| Sharing data with officials, coaches, volunteers to deliver training sessions or participate in events | Performance of a contract |
| Sharing data with Leagues, Divisional Associations, Irish FA to deliver the sport of football | Performance of a contract |
| Sharing data with committee members to provide information about community and social events | Legitimate interest for operational purposes |
| Sharing data with third party service providers or facility providers | Legitimate interest for operational purposes |
| Sharing data with a partner as a condition of funding | Legitimate interest for operational purposes |
| Sharing data with legal, statutory, regulatory bodies | Legal basis to comply with a legal obligation |
| Publishing match and league results | Consent to publish your personal data in a public domain including name and image. In the case of children under the age of 18 then only with written consent from parent/guardian |
| Sending out marketing information about promotions and offers from sponsors | Consent to send you direct marketing |
| Health and medical information | Consent to process details on your medical history including sharing information at the appropriate level |
| Processing children’s information | Performance of a contract in the case of children under the age of 18 with written consent from parent/guardian |

1. **Purpose Limitation**
   1. The Club/League/Divisional Association will only process personal data for the explicit and defined purposes of the Club/League/Divisional Association, or as permitted by the GDPR.
   2. You may only process personal data if required to do so in an official capacity with the Club/League/Divisional Association. The Club/League/Divisional Association cannot process personal data for any reason unrelated to its duties.
   3. The Club/League/Divisional Association must ensure that when personal data is no longer needed for the defined purposes, it is deleted or anonymised.
2. **Accurate data**
   1. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at the start of each season. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.
3. **Timely processing**
   1. We will not keep personal data longer than is necessary for the purpose(s) for which the data was collected. We will take all reasonable steps to destroy or delete data which is no longer required.
4. **Data security**
   1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
   2. We have proportionate procedures and technology to maintain the security of all personal data.
   3. Personal data will be transferred to another party to process on our behalf where we have a GDRP compliant written contract in place with that party.
   4. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data.
   5. Our security procedures include:

* + - Entry controls to premises where personal data is kept
    - Secure desks, cabinets, and cupboards. These should be locked if they hold personal data
    - Adequate and secure methods of disposal
    - Electronic devices must not show personal data to passers-by and should be locked when attended.
    - Anyone using personal electronic devices to access or process Club/League/Divisional Association personal data must have a password only access function, and should have appropriate anti-virus protection. These devices must have the Club/League/Divisional Association personal data removed prior to being replaced by a new device or prior to ceasing to work for, or on behalf of, the Club/League/Divisional Association.

1. **Reporting a personal data breach**
   1. In the case of a personal data breach, we may need to notify the data protection authority and the individual. The data protection authority for Northern Ireland is the Information Commissioner Office (ICO).
   2. If you know or suspect that a personal data breach has occurred, inform a member of the committee immediately, who may need to escalate to the League/Divisional Association/Irish FA. You should not delete or destroy any material or evidence relating to a potential breach.
2. **Data subject’s rights**
   1. All individuals, as data subjects, have rights under the GDPR including:
      * The right to be informed
      * The right to request access to any data held about them
      * The right to object to processing of their data
      * The right to have inaccurate or incomplete data rectified
      * The right to be forgotten (deletion or removal of personal data)
      * The right to restrict processing
      * The right to data portability
      * The right to not be subject to a decision which is based on automated processing
   2. The Club/League/Divisional Association is aware that any requests regarding the above should be immediately reported to the Committee/Board and where necessary escalated to the League/Divisional Association/Irish FA for guidance.
3. **Privacy Notices and Privacy Statements**
   1. At the point where we collect personal data we will inform the data subject of the defined purpose as to why we are collecting the data, and how and what we will be using the personal data for.
   2. The Club/League/Divisional Association Privacy Notice and Privacy Statements set out the lawful basis for processing personal data.
   3. Where we collect personal data directly from individuals, we will inform them about:
      * What personal data the Club/League/Divisional Association processes
      * Who the Club/League/Divisional Association collects personal data from
      * Why and on what lawful basis the Club/League/Divisional Association collects personal data
      * Who the personal data may be shared with
      * How long the Club/League/Divisional Association will hold the personal data for
      * Inform individuals of their rights under the GDPR
      * Inform individuals of the Club/League/Divisional Association processing activities.
   4. If we receive personal data about an individual from other sources, we will provide the above information to the individual as soon as possible and let them know who we received their personal data from.
   5. We will inform individuals whose data we process whether we are the data controller or data processor in regard to that data, and which individual(s) in the Club/League/Divisional Association are responsible for data protection.
4. **Subject Access Requests (SAR)**
   1. Individuals have the right to and may make a formal request for information we hold about them. Anyone who receives such a request should forward it to the Board/Committee immediately, and where necessary escalate the request to the League/Divisional Association/Irish FA for guidance.
   2. The Club/League/Divisional Association must deal with subject access requests within 30 days from the request being received.
   3. The Club/League/Divisional Association will only disclose personal data if we have checked the individual’s identity to make sure they are entitled to it.
5. **Consent**
   1. The Club/League/Divisional Association may process personal data by obtaining individual’s consent.
   2. An individual gives consent to processing their personal data if they clearly indicate specific and informed agreement to the processing, either by a statement or positive action.
   3. Individual’s must be able to withdraw consent at any time and the withdrawal must be carried out by the Club/League/Divisional Association.
   4. Explicit consent is usually required for processing special category personal data.
   5. Where children are involved then the consent must be in writing from the child’s parent/guardian.
   6. Where consent is our legal basis for processing, we will need to keep records of when and how this consent was captured.
6. **Special category data**
   1. Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. Information about an individual’s health is more sensitive, and so needs more protection.
   2. When processing special category personal data, additional protection and conditions must be met.
7. **Children’s data**
   1. When handling children’s personal data we give special consideration to safeguarding and data protection measures.
8. **Sharing personal information**
   1. We share personal data with Club/League/Divisional Association/Irish FA using IFA FMS.
   2. We may share personal data with third parties or suppliers for the services they provide and instruct them to process our personal data on our behalf. Where we share data with third parties, we will ensure we have a compliant written contract in place incorporating the minimum data protection terms as set out in the GDPR. This may be in the form of terms of service with the third party.
   3. We may share personal data we hold if we are under a duty to disclose or share personal data to comply with any legal obligations, or to enforce or apply any contract with the individual, to protect our rights, property, or safety of individuals working for or on behalf of the Club/League/Divisional Association or others.
9. **Transferring personal data to a country outside the EU**
   1. We may transfer personal data we hold to a country outside of the EU. We will do so only when provided with the assurance that sufficient data protection safeguards are in place to ensure the security of that personal data.
10. **Accountability**
    1. The Club/League/Divisional Association must implement appropriate technical and organisational measures to look after personal data, and is responsible for, and must be able to demonstrate compliance with the data protection principles.
    2. The Club/League/Divisional Association must have adequate resources and controls in place to document and to ensure GDPR compliance. These include providing privacy notice at all points of data capture, providing training on data protection and this policy, and regularly reviewing data protection measures.
11. **Changes to this policy**
    1. We reserve the right to change this policy at any time. Where appropriate we will communicate the changes to you.
12. **Responsibilities**
    1. The Club/League/Divisional Association Committee/Board will be responsible for ensuring compliance with this policy. Any queries about this policy or data protection matters should be referred to the Data Protection Officer (INSERT point of contact).