**Manchester Titans American Football Club**

**Data Protection Policy**

**Date Protection Act 2018**

**General Data Protection Regulation (GDPR)**

**Compliance Statement**

**The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018) GDPR**

**Introduction**

The ***EU General Data Protection Regulation (“GDPR”)*** brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. With the use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

**Our Commitment**

Manchester Titans American Football Club is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection.

We recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the new Data Protection Act 2018 (DPA 2018)

Manchester Titans American Football Club is dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation complying with the eight data protection principles Data protection principle:-s

* 1. Personal data shall be processed fairly and lawfully
* 2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
* 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
* 4. Personal data shall be accurate and, where necessary, kept up to date
* 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
* 6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018
* 7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
* 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Our objectives for GDPR compliance have been summarised in this statement and include the development and implementation of data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance. Manchester Titans American Football Club already has a consistent level of data protection and security across the club, however we are fully compliant with the GDPR 2018.

**Policies & Procedures**

Data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -

* ***Data Protection*** –

The main policy and procedure document for data protection meets the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

* ***Data Retention & Erasure*** –

Manchester Titans American Football Club will meet the *‘data minimisation’* and *‘storage limitation’* principles and ensure that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *‘Right to Erasure’* obligation and are aware of when this and other data subject’s rights apply; along with any exemptions, response timeframes and notification responsibilities.

* ***Data Breaches*** –

Manchester Titans American Football Club procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Ensuring that all members of staff are trained and fully aware of procedures and reporting measures.

* ***International Data Transfers & Third-Party Disclosures*** –

Manchester Titans American Football Club will not store or transfer personal information outside the EU. If under any exceptional reason that this would occur Manchester Titans American Football Club will ensure procedures and safeguarding measures are in place to secure, encrypt and maintain the integrity of the data.

* ***Subject Access Request (SAR)*** – Manchester Titans American Football Club will ensure that SAR procedures to provide the requested information and for making this provision free of charge.
* ***Legal Basis for Processing*** –

Manchester Titans American Football Club ensure all processing activities identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

* ***Privacy Notice/Policy*** –

Manchester Titans American Football Club Privacy Notice(s) will comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

* ***Obtaining Consent*** –

Manchester Titans American Football Club will require consent forms to be filled for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. Manchester Titans American Football Club has stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

* ***Direct Marketing*** –

Manchester Titans American Football Club will ensure that the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

* ***Data Protection Impact Assessments (DPIA)*** –

Where Manchester Titans American Football Club processes personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR’s Article 35 requirements. Manchester Titans American Football Club has implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

* ***Processor Agreements*** –

Manchester Titans American Football Club at present may use a third-party to process personal information on our behalf (*i.e, recruitment, Hosting, sponsorship)* however if this were to change Manchester Titans American Football Club will draft compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as Manchester Titans American Football Club*, meet and understand their/our GDPR obligations.

* ***Special Categories Data* –**

Where Manchester Titans American Football Club obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data.

Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature and date, with the right to modify or remove consent being clearly signposted.

**Data Subject Rights**

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide information regarding an individual’s right to access any personal information that Manchester Titans American Football Clubprocesses about them and to request information about: -

* What personal data we hold about them
* The purposes of the processing
* The categories of personal data concerned
* The recipients to whom the personal data has/will be disclosed
* How long we intend to store your personal data for
* If we did not collect the data directly from them, information about the source
* The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
* The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
* The right to lodge a complaint or seek judicial remedy and who to contact in such instances

**Information Security & Technical and Organisational Measures**

Manchester Titans American Football Club takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process.

We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

Password protection, encryptions, pseudonymisation, IT restrictions, authentication.

**GDPR Roles and Employees**

The Secretary at Manchester Titans American Football Club is the designated Data Protection Officer (DPO)and will ensure that compliance with the new data protection Regulation. Promoting awareness of the GDPR across the club.

Manchester Titans American Football Club understands that continuous member awareness and understanding is vital to the continued compliance of the GDPR.

**Data Protection Impact Assessments (DPIA**)

**Data Protection Impact Assessment &**

**Form**

# Introduction

This Data Protection Impact Assessment (hereafter, “DPIA”), describes how Manchester Titans American Football Club uses of additional administrative measures to safeguard and protect personal information relating to members. The protection of personal information is something Manchester Titans American Football Club takes very seriously***.***

At Manchester Titans American Football Club all members have an expectation that their privacy and confidentiality will be respected at all times. It is essential consequently that when Manchester Titans American Football Club is contemplating or implementing any new initiatives which involves the use of technology, the perceived impact of collection, use and disclosure of any personal data is considered integral to an individual’s privacy. Carrying out a Data Protection Impact Assessment (DPIA) is a disciplined way of achieving this objective.

# Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process that helps Manchester Titans American Football Club identify risks to the privacy of data subjects and ensure legitimate best practice are followed when a new project is planned. The purpose DPIA serves is to ensure that privacy related risks that arise during data collection, use and disclosure are mitigated using appropriate plans and measures, while allowing the objectives which involves the use of personal data, to be met.

# What are Privacy Risks?

A privacy risk can be defined as the probability that the fundamental rights and freedom of a data subject may be put at risk through the data processing activities of Manchester Titans American Football Club. Privacy related risks can include one or all of the following:

* Risks to members other third parties (for example, loss of anonymity, intrusion into the private lives through monitoring activities, lack of transparency, fairness and lawfulness of data processing activities etc.).
* Compliance risks e.g. breach of the General Data Protection Regulation, BAFA regulations UK Laws.
* Inherent or residual risks to Manchester Titans American Football Club (for example:- legal penalties or claims, damage to Manchester Titans American Football Club reputation, loss of trust from members).

## Members Perspective

DPIAs helps Manchester Titans American Football Club see things from the data subject’s perspective. How patient data is used and why it will be used should be clearly outlined and articulated and where appropriate, requires that consent is sought, given, maintained and sustained.

Understanding the potential impact of personal data processing on individuals can enable systems to be designed around data subject’s legal rights and expectations of confidentiality as outlined under the new regulation. This phenomenon is known as data protection by design and default.

A DPIA also checks organisational compliance against legal framework (where relevant). A lead person should coordinate and lead the DPIA process.

# Data Privacy Impact Assessment Form

|  |  |
| --- | --- |
| **Name of Assessor** |  |
| **Position in Club** |  |
| **Date completed** |  |
| **Phone/Mobile** |  |
| **E-mail** |  |
| What is it that is being planned? | |
|  | |
| **Purpose / Objectives:** Why is DPIA it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project. | |
|  | |
| **What is the purpose of collecting the information within the system?** For example research, reporting, funding information requirements. | |
|  | |
| **What are the potential privacy impacts of this proposal**? How will this change impact upon the member?  Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing. | |
|  | |
| **Committee members:** Who is involved in this project? Please list members internal, external, organisations (public/private/third) and groups that may be affected. | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **What data is being collected, shared or used?** | | | |
|  | **Data Type** | | **Justifications –** there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project? |
| **Information that identifies the individual and their personal characteristics** | Name | ☐ |  |
| Address | ☐ |
| Postcode | ☐ |
| Dob | ☐ |
| Age | ☐ |
| Gender | ☐ |
| Racial/ethnic origin | ☐ |
| Mobile/home phone no. | ☐ |
| Email address | ☐ |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **N/A** | **Justification** |
| Information relating to the individual’s physical or mental health or condition. | ☐ | ☐ |  |
| Information relating to the family of the individual and the individual’s lifestyle and social circumstances | ☐ | ☐ |  |
| Information relating to any offences committed or alleged to be committed by the individual | ☐ | ☐ |  |
| Information relating to criminal proceedings, outcomes and sentences regarding the individual | ☐ | ☐ |  |
| Employment and career history. | ☐ | ☐ |  |
| Information relating to the individual’s membership payments. | ☐ | ☐ |  |
|  | ☐ | ☐ |  |
| Will the information be   1. Anonymised | ☐ | ☐ |  |
| 1. Pseudonymised | ☐ | ☐ |
| 1. Identifiable | ☐ | ☐ |
| Select the appropriate choice. Please note that where possible information should be anonymised |  |  |

**Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Question** | **Response** | **Required Action**  **E.g. Seek Information Governance advice** |
| **Legal compliance – is it fair and lawful?** | 1. What is the legal basis for processing the information? This is your valid legal reason for processing. |  |  |
| 1. Is the processing necessary and proportionate if the legal basis is Article 6(1)(f) “legitimate interests”? If the answer is “no” processing should not proceed. |  |  |
| 1. a) - Is the processing of individual’s information likely to interfere with the ‘right to privacy’ under Article 8 of the Human Rights Act? |  |  |
| 1. It is important that members affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed? |  |  |
| 1. If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn? |  |  |
| **Purpose** | 1. Does the project involve the use of existing personal data for new purposes? |  |  |
| 1. Are potential new purposes likely to be identified as the scope of the project expands? |  |  |
| **Adequacy** | 1. Is the information you are using likely to be of good enough quality for the purposes it is used for? |  |  |
| **Accurate and up to date** | 1. Are you able to amend information when necessary to ensure accuracy? |  |  |
| 1. How are you ensuring that personal data obtained from individuals or other organisations is accurate? |  |  |
| **Retention** | 1. What are the retention periods for the personal data and how will this be implemented? |  |  |
| 1. Are there any exceptional circumstances for retaining certain personal data for longer than is necessary? |  |  |
| 1. How will personal data be fully anonymised or destroyed after it is no longer necessary or fit for purpose? |  |  |
| **Rights of the individual** | 1. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? Will the information be provided to the data subject on their right to rectification, erasure, portability etc? |  |  |
| **Appropriate technical and organisational measures** | 1. What procedures are in place to ensure that all committee members with access to the members data have received adequate information governance training? |  |  |
| 1. If using an electronic system to process subject access requests, what security measures are in place? |  |  |
| 1. How will the information be provided, collated and used? |  |  |
| 1. What security measures will be used to transfer the identifiable information? 2. Have you identified any potential risk? 3. The potential impact of any such risk on the data subject. 4. The likelihood and severity of any risk. 5. How you intend to deal with it. |  |  |
| **Transfers both internal and external including outside of the EEA** | 1. Will individual’s personal information be disclosed internally/externally in identifiable form and if so to whom, how and why? |  |  |
| 1. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data? |  |  |
| **Consultation** | 1. Who should be consulted to identify privacy related risks and how will this be achieved? |  |  |
| 1. Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc. |  |  |
| **Guidance used** | 1. List any national guidance applicable to the initiative that is referred to. |  |  |

## Privacy issues identified and risk analysis

### Identify the privacy and related risks

Allocate a reference number to each identified privacy issue to link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column

*TABLE 1*

|  | **Privacy issue –** element of the initiative that gives rise to the risk | 1. **Risk to individuals**   (complete if appropriate to issue or put not applicable) | 1. **Compliance risk**   (complete if appropriate to issue or put not applicable) | 1. **Club risk**   (complete if appropriate to issue or put not applicable) |
| --- | --- | --- | --- | --- |
| *PR1* | *Individuals are not aware of the initiative as no communication materials have been planned* | *Individuals not aware that their data is being processed* | *Non-compliance with Article 5(1) principle /Concept 1 – fairness, lawfulness and transparency* | 1. *May lead to public mistrust* 2. *May lead to sanction by BAFA* |
|  |  |  |  |  |

### Identify the privacy solutions

*Table 2*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Risk – taken from column (a), (b) and/or (c) in table 1.** | **Risk score –** | | | **Proposed solution(s)**  **/mitigating action(s)** | **Result: is the risk accepted, eliminated, or reduced?** | **Risk to individuals is now OK?**  **Signed off by?** |
| **Likelihood** | **Impact** | **status** |  |  |  |
| *PR1* | *Individuals not aware that their data is being processed*  *Non-compliance with DPA principle 1 – fair and lawful processing*  *1. May lead to public mistrust*  *2. May lead to sanction by BAFA* | 5 | 5 |  | *Communication plan to be developed to ensure compliance with fair and lawful processing*  *Assurance that there will be active communication*  *Committee members informed of need to understand and disseminate communication material.* | *Reduced to an acceptable level (it is not possible to eliminate at this stage as the Comms plan will need to ensure it addresses all aspects to enable individuals to be fully informed.* | *Yes*  *Sign-off tbc* |
|  |  |  |  |  |  |  |  |

### Integrate the PIA outcomes back into the project plan

This must include any actions identified in Table 1 and Table 2.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Who is responsible for integrating the outcomes back in to the project**  **Who is responsible for implementing the solutions that have been approved?**  **Who is the contact for any privacy concerns which may arise in the future?** | | | | | | | |
| **Ref No.** | **Action to be taken** | **Date for completion of actions** | **Anticipated risk score following mitigation** | | | **Responsibility for action – *job title not names*** | **Current status/progress** |
| **Likelihood** | **Impact** | **RAG status** |
| *PR1* | *Communications plan to be developed* |  | *2* | *2* |  | *Secretary to liaise with Communication lead* | *Meeting arranged with appropriate committee member* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Types of privacy risk**

## Risks to individuals

* Inadequate disclosure controls increase of information being shared inappropriately.
* The context in which information is used or disclosed can change over time, or being used for different purposes without people’s knowledge.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing of datasets can allow organisations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or disclosure of information.
* Collecting information and linking identifiers might mean that Manchester Titans American football club is no longer using information which is safely anonymised.
* Information which is collected and stored unnecessarily presents a greater security risk.
* Retention period is not established and might be used for longer than necessary.

## Compliance Risk

1. Non-compliance with the common law duty of confidentiality
2. Non-compliance with the Data Protection Acts 2018/ General Data Protection Regulation (GDPR).
3. Non-compliance with the Privacy and Electronic Communications Regulations (PECR)/e-Privacy Regulation.
4. Non-compliance with BAFA rules and regulations
5. Non-compliance with human rights legislation United Nations Declaration on human Rights (UNDHR).

## Associated Club risk

1. Non-compliance with the IDPA or other legislation can lead to sanctions, fines and reputational damage.
2. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the club.
3. Public distrust about how information is used can damage Manchester Titan American football club’s reputation and lead to loss of members.
4. Data losses which damage individuals could lead to claims for compensation.

**Guidance for completing a risk register**

* What is the actual risk? Make sure the risk is clear and concise, well understood and articulated with appropriate use of language, suitable for the public domain.
* Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests.
* Don’t reference blame to other organisations in the risk register

RAG stands for red, amber and green. To achieve a RAG rating, each risk needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

**Likelihood**



**Impact**



Using the “RAG” system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

A

A/R

R

R

R

A

A

A/R

R

R

A/G

A

A

A/R

A/R

Very High -5

High - 4

Medium - 3

G

A/G

A/G

A

A

G

G

G

G

G

1

Rare

2

Unlikely

3

Possible

4

Likely

5

Almost Certain

**Likelihood**

Low - 2

Very Low - 1

**Impact**