PLYMOUTH ARENA

PERSONAL DATA PROTECTION POLICY

VERSION: 2.0

DATE: 06/11/2025

REFERENCE NUMBER: PA/IND12/2025/PDPP

RESPONSIBLE PERSON: DATA PROTECTION GROUP (DPA)

DATE FOR RENEWAL: JULY 2026

ICONIC.
INDEPENDENT.
YOURS.

PERSONAL DATA PROTECTION POLICY

PURPOSE

Plymouth Arena hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Company operates.

SCOPE

This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

POLICY

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of The Company.

ENFORCEMENT

The Audit Department or other relevant department is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to a civil or criminal liabilities if his or her conduct violates laws or regulations.

PROCEDURE

The data protection principles outline the basic responsibilities and procedures for handling personal data. Article 5(2) of the GDPR stipulates that “*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*.”

This Policy specifies the basic principles regarding personal data processing.

1. PURPOSE, SCOPE AND USERS

Plymouth Arena hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Company operates. This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of The Company.

Reference Documents

UK GDPR is the retained EU law version of the GDPR, as it forms part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as supplemented by the Data Protection Act 2018.

The Data Protection Act 2018 (UK) & UK GDPR

Processor GDPR Compliance Questionnaire

Supplier Data Processing Agreement

Data Subject Access Request Procedure

Data Protection Impact Assessment Methodology

Register of Privacy Notices

Data Breach Response and Notification Procedure

Definitions

The following definitions of terms used in this document are drawn from UK GDPR (Article 6):

Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data: Personal data which is, by its nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of its processing could create significant risks to the fundamental rights and freedoms of data subject. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymisation: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymised data as it is no longer personal data.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. Pseudonymisation reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymised data is still personal data, the processing of pseudonymised data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

Supervisory Authority: An independent public authority which is established by a Member State pursuant to Article 51 of the UK GDPR

Lead supervisory authority: The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority in regards to its duties to ensure compliance with the provisions of the UK GDPR;

Each "**local supervisory authority**" will still maintain its own territory and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers include conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

"Main establishment as regards a controller" with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the

latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

"Main establishment as regards a processor" with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

Group Undertaking: Any holding company together with its subsidiary.

BASIC PRINCIPLES REGARDING DATA PROTECTION

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.2 PURPOSE LIMITATION

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3 DATA MINIMISATION

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. The Company must apply Anonymisation or Pseudonymisation to personal data if possible to reduce the risks to the data subjects concerned.

4.4 ACCURACY

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified in a timely manner.

4.5 STORAGE PERIOD LIMITATION

Personal data must be kept for no longer than is necessary for the purposes for which the personal data is processed.

4.6 INTEGRITY AND CONFIDENTIALITY

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Company must use appropriate technical or organisational measures to process Personal Data in a manner that ensures appropriate security of

personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorised access to, or disclosure.

4.7 ACCOUNTABILITY

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

BUILDING DATA PROTECTION IN BUSINESS ACTIVITIES

In order to demonstrate compliance with the principles of data protection, an organisation should build data protection into its business activities.

5.1 NOTIFICATION TO DATE SUBJECTS

(See the Fair Processing Guidelines section.)

5.2 DATA SUBJECTS CHOICE AND CONSENT

(See the Fair Processing Guidelines section.)

5.3 COLLECTION

The Company must strive to collect the least amount of personal data possible. If personal data is collected from a third party, GDPR responsible person must ensure that the personal data is collected lawfully.

5.4 USE, RETENTION AND DISPOSAL

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in the Privacy Notice. The Company must maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. GDPR responsible person is responsible for compliance with the requirements listed in this section.

5.5 DISCLOSURE TO THIRD PARTIES

Whenever the Company uses a third-party supplier or business partner to process personal data on its behalf, GDPR responsible person must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, the Processor GDPR Compliance Questionnaire must be used.

The Company must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes. When the Company processes personal data jointly with an independent third party, the Company must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

5.6 CROSS-BORDER TRANSFER OF PERSONAL DATA

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorisation from the relevant Data Protection Authority must be obtained. The entity receiving the personal data must comply with the principles of personal data processing set forth in Cross Border Data Transfer Procedure.

5.7 RIGHTS OF ACCESS BY DATA SUBJECTS

When acting as a data controller, GDPR responsible person is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

DATA PORTABILITY

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit this data to another controller, for free. GDPR responsible person has to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

5.9 RIGHT TO BE FORGOTTEN

Upon request, Data Subjects have the right to obtain from the Company the erasure of its personal data. When the Company is acting as a Controller, GDPR responsible person must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

FAIR PROCESSING GUIDELINES

Personal data must only be processed when explicitly authorised by GDPR responsible person.

The Company must decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

6.1 NOTICES TO DATA SUBJECTS

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, GDPR responsible person is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and

the Company's security measures to protect personal data. This information is provided through Privacy Notice.

Where personal data is being shared with a third party, GDPR responsible person must ensure that data subjects have been notified of this through Privacy Notice.

Where personal data is being transferred to a third country according to Cross Border Data Transfer Procedure, the Privacy Notice should reflect this and clearly state to where, and to which entity personal data is being transferred.

Where sensitive personal data is being collected, the GDPR responsible person must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

6.2 OBTAINING CONSENTS

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, GDPR responsible person is responsible for retaining a record of such consent. GDPR responsible person is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

When requests are received to correct, amend or destroy personal data records, GDPR responsible person must ensure that these requests are handled within a reasonable time frame. GDPR responsible person must also record the requests and keep a log of these.

Personal data must only be processed for the purpose for which it was originally collected. In the event that the Company wants to process collected personal data for another purpose, the Company must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). GDPR responsible person is responsible for complying with the rules in this paragraph.

Now and in the future, GDPR responsible person must ensure that collection methods are compliant with relevant law, good practices and industry standards.

GDPR responsible person is responsible for creating and maintaining a Register of the Privacy Notices.

5 ORGANISATION AND RESPONSIBILITIES

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with the Company and has access to personal data processed by the Company.

The key areas of responsibilities for processing personal data lie with the following organisational roles:

The board of directors or other relevant decision-making body such as the Chief Executive, makes decisions about, and approves the Company's general strategies on personal data protection.

The Data Protection Administrator along with the appointed **Data Protection Officer** is responsible for managing the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies.

The **Facilities Director/Information Security Officer/IT Services Provider** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The Client Services Manager, along with Marketing Executives, is responsible for:

Approving any data protection statements attached to communications such as emails and letters.

Addressing any data protection queries from journalists or media outlets like newspapers.

Where necessary, working with the GDPR responsible person to ensure marketing initiatives abide by data protection principles.

The Office Administrator along with the Data Protection Administrator is responsible for:

Improving all employees' awareness of user personal data protection.

Organising Personal data protection expertise and awareness training for employees working with personal data.

End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

In addition to the above, Departmental Managers along with the Data Protection Administrator are responsible for passing on personal data protection responsibilities to suppliers and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using. The Procurement Department, or person/s with similar responsibilities must ensure that the Company reserves a right to audit suppliers.

GUIDELINES FOR ESTABLISHING THE LEAD SUPERVISORY AUTHORITY

8.1 NECESSITY TO ESTABLISH THE LEAD SUPERVISORY AUTHORITY

Identifying a Lead supervisory authority is only relevant if the Company carries out the cross-border processing of personal data.

Cross border of personal data is carried out if:

a) processing of personal data is carried out by subsidiaries of the Company which are based in other Member States;

or

b) processing of personal data which takes place in a single establishment of the Company in the European Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

If the Company only has establishments in one Member State and its processing activities are affecting only data subjects in that Member State than there is no need to establish a lead supervisory authority. The only competent authority will be the Supervisory Authority in the country where Company is lawfully established.

8.2 MAIN ESTABLISHMENT AND THE LEAD SUPERVISORY AUTHORITY

8.2.1 MAIN ESTABLISHMENT FOR THE DATA CONTROLLER

The top management of the Company needs to identify the main establishment so that the lead supervisory authority can be determined.

If the Company is based in an EU Member State and it makes decisions related to cross-border processing activities in the place of its headquarters there will be a single lead supervisory authority for the data processing activities carried out by the Company.

If Company has multiple establishments that act independently and make decisions about the purposes and means of the processing of personal data top management of the Company needs to acknowledge that more than one lead supervisory authority exists.

8.2.2 MAIN ESTABLISHMENT FOR THE DATA PROCESSOR

When the Company is acting as a data processor, then the main establishment will be the place of central administration. In case the place of central administration is not located in the EU, the main establishment will be the establishment in the EU where the main processing activities take place.

8.2.3 MAIN ESTABLISHMENT FOR NON-EU COMPANIES FOR DATA CONTROLLERS

If the Company does not have a main establishment in the EU, and it has subsidiaries in the EU, then the competent supervisory authority is the local supervisory authority.

If the Company does not have a main establishment in the EU nor the subsidiaries in the EU, it must appoint a representative in the EU, and the competent supervisory authority will be the local supervisory authority where the representative is located.

6 RESPONSE TO PERSONAL DATA BREACH INCIDENTS

When the Company learns of a suspected or actual personal data breach, GDPR responsible person must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach Response and Notification Procedure. Where there is any risk to the rights and freedoms of data subjects, the Company must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

7 AUDIT AND ACCOUNTABILITY

The Audit Department or other relevant department is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

CONFLICTS OF LAW

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which PLYMOUTH ARENA operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Subject Consent Forms	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the forms	10 years
Data Subject Consent Withdrawal Form	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the forms	10 years
Supplier Data Processing Agreements	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the folder	5 years after the agreement has expired
Register of Privacy Notices	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the folder	Permanently
Cross Border Data Transfer Procedure	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the folder	Permanently

Processor GDPR Compliance Questionnaire	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the folder	5 years after the agreement has expired
Data Protection Impact Assessment Guidelines	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the folder	Permanently
Data Breach Response and Notification Procedure	I:\global policies & procedures\GDPR\GDPR	GDPR responsible person	Only authorised persons may access the folder	Permanently

VALIDITY AND DOCUMENT MAN AGENT

This document is valid as of 25/04/2019.

The owner of this document is GDPR responsible person, who must check and, if necessary, update the document at least once a year.