Reading Football Supporters' Society Limited,
Registered Office: c/o Vale & West, Victoria House
26 Queen Victoria Street, Reading. RG1 1TG.

www.star-reading.org

The STAR Data Protection Policy

Date of Review	Reason for Review	Amendments
10th May 2018	New GDPR Legislation	Full Re-Write

1.Introduction

This document is drafted in accordance with the Rules of Reading Football Supporters' Society Limited and sets out the Policy towards the General Data Protection Regulation (GDPR). It outlines STAR's obligations under GDPR (approved by the EU Parliament on 14 April 2016 with an enforcement date of 25 May 2018), which sets standards that STAR must meet when obtaining, recording, holding, using or disposing of data on behalf of its members. The accompanying Appendix A details how STAR will meet the requirements when processing any Personal Data on behalf of its members, suppliers and contractors. Appendix B contains the STAR personal data Privacy Policy that will be shared with all members on who subscribe to STAR membership. Appendix C contains the STAR Membership Data Retention Guidelines. Appendix D contains a glossary of GDPR terms.

2.Definitions

Definitions of the terms used in this policy are laid out in a separate Definition of Terms document, which should be read in conjunction with this Policy.

3.Scope

This Policy applies to all STAR Board members and other persons who process data on behalf of STAR in accordance with STAR's personal data Privacy Policy.

4. Responsibilities

The STAR Board is ultimately accountable for adherence to legal requirements, society policies, standards and procedures, and overseeing any proceedings which may result from any non-compliance with this Policy. The STAR Data Controller is the person with delegated responsibility for STAR' personal data Privacy Policy. The Society Secretary will assist in this remit, together with answering queries. It is the responsibility of all Board members to ensure that other persons undertaking tasks in the areas of STAR's operations or activities for which they are responsible are fully conversant with their Data Protection responsibilities. Instructions combined with training will be provided for all new and existing Board members, Team members and other persons. All Board members and other persons, who process data on behalf of STAR must, in accordance with STAR's personal data Privacy Policy, comply with their Data Protection responsibilities.

5. Failure to comply with this Policy

STAR has a legal and moral duty to protect the personal data with which it is entrusted. Failure of those listed in paragraph 4 above to comply with this Policy may result in sanctions being taken against them.

Fines for non-compliance to GDPR can be up to: €20m or 4% of turnover. Non-compliance includes failing to respond to data requests from members in a timely manner, data breaches, through to infringement of an individual's privacy policy.

6. Control procedures in place

The Data Controller will ensure that all persons who process personal data on behalf of STAR will be given instruction so that they are made fully aware of their responsibility as per GDPR legislation, and to escalate any concerns about data management to the Data Controller. If such a concern is raised, an investigation will be made, and corrective action taken as appropriate.

7. Charging

The previous £10 administration fee to fulfill Subject Access Requests (defined in the Data Protection Act 1998) has been abolished. Although "reasonable" fees can be charged for manifestly unfounded or excessive requests.

8. Responsibility for monitoring this Policy

The responsibility for monitoring this Policy rests with the Society's Board which will review the Policy annually.

Appendix A: The General Data Protection Regulation (GDPR) 2018

What is The General Data Protection Regulation (GDPR) 2018)?

It sets the standards that must be satisfied when obtaining, recording, holding, using or disposing of personal data. The GDPR applies to those who handle or have access on behalf of STAR to information about individuals. It also gives rights to the people the information is about. Everyone who has STAR's data has a legal duty to protect the privacy of information about individuals. Failure to comply with STAR's Data Protection Policy may result in sanctions being taken against the individual concerned.

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Key GDPR Roles

The Data Controller: is responsible for determining the purpose, conditions and means of processing of personal data: defining the STAR Data Protection Policy, including the Privacy Policy. Answering queries and ensuring that STAR's data protection policies and procedures are communicated as required. The Society Secretary assists in this role.

Data Processor - the entity that processes data on behalf of the Data Controller – i.e. STAR board members and its suppliers.
Data Subject - a natural person whose personal data is processed by a controller or processor – i.e. STAR members and other persons whose duties and activities involve processing personal information.

Data Protection Officer - This role is not required for STAR (not a public body, have low scale personal data processing and low requirement for systematic monitoring of data subjects).

What information does the GDPR apply to?

- ### Personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

- ### Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" - data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

STAR do not hold any sensitive personal data.

What are the main principles of GDPR?

GDPR is based on six data protection principles as detailed below:

1. Lawfulness, fairness and transparency

Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)].

Personal data can only processed in line with the STAR personal data Privacy Policy.

2. Purpose limitations

Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Personal data can only be used for the purposes explicitly stated in the STAR personal data privacy policy.

3. Data minimisation

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing.

Information that is not relevant for the purpose must not be collected simply because it might be useful in the future. Avoid abbreviations, use clear, legible writing, stick to the facts and do not add personal opinions and comments.

4. Accuracy

Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

Take care when inputting information to ensure accuracy. Avoid creating duplicate records as these can get out of alignment when being updated.

5. Storage limitations

Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. In summary, data no longer required should be removed.

Appendix C defines the STAR policy for personal data retention. Personal data cannot be kept in case it might be useful one day. A formal record of personal data deletion will be maintained by the STAR membership secretary.

6. Integrity and confidentiality

Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)].

STAR's security measures to prevent unauthorised access include the following restrictions and precautions:

Physical security controls, physical copies of personal data shall be stored in locked cupboards in locked rooms (e.g. STAR base or home).

Electronic storage of personal data, shall be password protected and encrypted. The password will meet secure standards (8 digits, with a mix of Capital, Lower case, numbers and symbols) and be changed every three months. The password will be communicated to any STAR Board member using the data, using a different media than is used to send the data (e.g. email the data, text the password).

Memory sticks shall only be used in exceptional circumstances to communicate the encrypted/password protected data file. In this case full focus and care must be taken not to lose the memory stick, or leave around for others to copy.

The passwords for the 3 systems used by STAR (MailChimp. Paypal and ECWID) shall be securely stored and not shared with any other STAR board member who does not require access to these tools. If a STAR board member who has access to any of these systems, leaves the board – the relevant password shall be changed immediately.

In addition GDPR provides the following rights for individuals:

1. The right to be informed

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.

2. The right of access

- Individuals have the right to access their personal data and supplementary information.
- The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3. The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.

4. The right to erasure

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

5. The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21)

6. The right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. The right to object

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling.

- The GDPR has provisions on:
- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

STAR has 30 days to respond to a Subject Access Request (SAR) from members on the personal data that STAR holds on them.

Appendix B: The STAR personal data Privacy Policy

STAR treats the privacy of members and website viewers very seriously and we take appropriate security measures to protect your privacy. This privacy policy explains how we collect, manage and protect your personal data during you STAR membership.

Personal data means any information relating to an identifiable person (e.g. first and last name, address or email) that may be used directly or indirectly to identify and individual.

How we obtain your personal data

You provide us your personal data during membership renewal and any subsequent interaction during the membership year and subsequent three-month renewal period.
We do not seek or secure any additional information from other sources.

How we use your personal data

We use your personal data to manage your membership, including communicating relevant information to you (Event Information, STAR Bulletins, Membership Information) during the membership year. We undertake to protect your data and take reasonable measure to protect your personal data in storage.
We do not share or use your personal data for marketing purposes.

We share your Reading FC Customer Number, Name and post code with Reading FC, to secure your 20 bonus Loyalty Points. Reading FC already hold this data, subject to the Reading FC Privacy Policy between you and them. Reading FC do not make any further use of this data shared by STAR.

Information about cookies

A cookie is a small text file on your browser (e.g. Google Chrome). The STAR policy on management of cookies can be found at: http://star-reading.org/index.php/cookies/

Providing your personal data to others

STAR uses three third party systems (not relevant to all members) in managing your STAR membership:
MailChimp (used for STAR Bulletins and other email communication). MailChimp have updated their privacy policy to bring it line with the General Data Protection Regulation (GDPR). Mailchimp uses servers located in the United States (and so personal data is transferred outside the EU) but takes steps to protect your privacy in line with the GDPR.

Paypal (used for online membership and online shop payments). Paypal transactions are subject to the Paypal Privacy Policy, which has recently been amended to bring it line with the General Data Protection Regulation.

ECWID (online shop used for pilot online travel booking). Ecwid has followed GDPR guidelines on data collection, storage, processing and sharing personal data. They have many customers in Europe, and they work hard to meet all legal requirements. Ecwid uses secure data servers based in Europe, and all sensitive data is transferred via secure HTTPS protocol.

How long do we keep information?

We keep your information as follows:

- During and up to 3 months after the current membership year expires (i.e. to the end of September) for communicating relevant information to you (Event Information, STAR Bulletins, Membership Information).
- For a full 12 months after the current membership year, solely for processing membership renewals.
- If you formally agree on the membership form/renewal ("To continue receiving communication from us after this year's membership expires tick here"), for 24 months after the current membership year expires for communicating relevant information to you (Event Information, STAR Bulletins, Membership Information).

International transfers of your personal data

We do not currently transfer your data outside the EEA, except for your email address, which our email service provider MailChimp as described above, hosts in the USA. If this changes we will update you and this policy.

Data subject rights

Subject access requests

GDPR grants you permission to access the personal data we hold on you.

Right to rectification

You have the right to have any inaccurate person data, rectified, without undue delay.

Right to erasure

You have the right to have your data erased, without undue delay.

Right to restriction of processing

You have the right to restrict processing of your data, without undue delay.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

We shall secure, where possible, confirmation from all related parties of any requested rectification, erasure or restriction of your personal data.

Right to data portability

You have the right to receive your data in a commonly used and Machine-Readable format.

Right to object

You have the right to object to the processing of personal data concerning you. The services we provide to you, may be limited from this action.

Right to not be subject of decisions based on automated processing

We do not carry out any automated processing of your personal data.

Important Information

Questions, queries and complaints.

If you have any questions, queries or complaints on this policy, or the personal data that we hold, please email us on onlinemembership@star-reading.org.

Policy Changes

This policy will be reviewed annually and will be updated on the STAR web-site star-reading.org. In addition, the latest version will be provided at the start of every new membership year.

Appendix C: STAR Membership Data Retention Guidelines

STAR will retain data in line with GDPR and the Data Policy, with the following specific guidelines:

• Membership Data will be retained for 3 months after the end of the membership year – solely for general communication (e.g. STAR Bulletins) and email marketing contact to encourage membership renewal.

• Membership Data will be retained for 12 months after the end of the membership year – solely for member lead membership renewals, re-using contact and address information.

• Membership Data will be retained for 24 months after the end of membership year, for those who have ticked this preference on the membership form/online application, solely for general communication and email marketing contact to encourage membership renewals.

Appendix D: GDPR Glossary of Terms

A Glossary of Terms and Definitions as used in relation to the GDPR.

Binding Corporate Rules (BCRs)- a set of binding rules put in place to allow multinational companies and organisations to transfer personal data that they control from the EU to their affiliates outside the EU (but within the organisation)

Biometric Data - any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification

Consent- freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

Data Concerning Health - any personal data related to the physical or mental health of an individual or the provision of health services to them

Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data

Data Erasure - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Data Portability - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller (more info here)

Data Processor - the entity that processes data on behalf of the Data Controller

Data Protection Authority - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Officer - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR (more info here)

Data Subject - a natural person whose personal data is processed by a controller or processor

Delegated Acts - non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity

Derogation - an exemption from a law

Directive - a legislative act that sets out a goal that all EU countries must achieve through their own national laws

Encrypted Data - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Enterprise - any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

Filing System - any specific set of personal data that is accessible according to specific criteria, or able to be queried

Genetic Data - data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual

Group of Undertakings - a controlling undertaking and its controlled undertakings

Main Establishment - the place within the Union that the main decisions surrounding data processing are made; with regard to the processor

Personal Data - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Personal Data Breach - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

Privacy Impact Assessment - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

Pseudonymisation - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution

Recipient - entity to which the personal data are disclosed

Regulation - a binding legislative act that must be applied in its entirety across the Union

Representative - any person in the Union explicitly designated by the controller to be addressed by the supervisory authorities

Right to be Forgotten - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

Right to Access - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Subject Access Right - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

Supervisory Authority - a public authority which is established by a member state in accordance with article 46

Trilogues - informal negotiations between the European Commission, the European Parliament, and the Council of the European Union usually held following the first readings of proposed legislation in order to more quickly agree to a compromise text to be adopted.