FIFA®

Data Protection Regulations

October 2019 edition

Fédération Internationale de Football Association

President:	Gianni Infantino
Secretary General:	Fatma Samoura
Address:	FIFA FIFA-Strasse 20 P.O. Box 8044 Zurich Switzerland
Telephone:	+41 (0)43 222 7777
Internet:	FIFA.com

FIFA Data Protection Regulations

October 2019 edition

CONTENTS *Page*

1 Preamble 4
2 Definitions 4
3 Scope 7
4 Data Processing 8
1. Principles 8
2. Special Categories of Personal Data 9
5 Data Subject's rights 10
6 Transmission of Personal Data to Third Parties/Data Processing by Third Parties 12
7 Cross-border Disclosure 12
1. Principles 12
2. Lack of an adequate level of data protection abroad 12
8 Entity-internal Processing guidelines 13
1. Responsibilities 13
2. Process Owner 13
3. Data inventory 13
4. Checks by the Process Owner 13
9 Information security requirements 14
10 Data Security Incidents 14
11 Data Protection Officer (DPO) 14
12 Final provisions 15
1. Official languages 15
2. Sanctions 15
3. Entry into force 15

NB: References to natural persons include both genders. For the sake of simplicity, only the masculine form has been used. All references in the singular are also applicable in the plural and vice-versa.

1 Preamble

FIFA is committed to respecting the individual rights of every person with whom it interacts, and therefore the protection of Personal Data is of great importance. These Regulations define Data Processing principles, data transfers within and between FIFA, its Member Associations and any Entities to which these Regulations are applicable, the standard for protecting Special Categories of Personal Data, and the rights of all Data Subjects.
FIFA's operations include the Processing of various types of Personal Data. With these Regulations, FIFA pursues the following objectives:

- Establishment of a standard to be applied when Processing Personal Data
- Providing preventive safeguards against the infringement of personality and privacy rights through the inappropriate Processing of Personal Data

These Regulations apply in addition to the Applicable Data Protection Laws. Compliance with the latter must be achieved, especially where the Applicable Data Protection Laws are stricter than the principles set out in these Regulations.

2 Definitions

The following definitions (initial capitals) shall apply within these Regulations:

Applicable Data Protection Laws
The Swiss Federal Act on Data Protection (FADP), and, where applicable to a specific Processing of Personal Data, any other applicable data protection laws, each as amended from time to time.

Consent
Any freely given, specific, informed and unambiguous indication of the Data Subjects' wishes by which they, by a statement or by a clear affirmation, signify agreement to the Processing of Personal Data relating to them.

Data Security Incident
Any event of loss of confidentiality, integrity and availability with the potential of constituting a risk for FIFA, any other Entity or any Data Subject.

Data Subject
An identified or identifiable natural person about whom data is processed. An identifiable natural person is one who can be identified or singled out, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Disclosure / to disclose
The transmission of Personal Data or provision of access to Personal Data, e.g. by making it available for inspection, transferring it or publishing it.

Entity Unit
"Entity" means FIFA, any Member Association, or any of the latter's members. "Unit" means any single hierarchical element of an Entity's internal organisation.

FADP
The Swiss Federal Act on Data Protection of 19 June 1992 (index no. 235.1), as amended from time to time.

FDPIC
The Federal Data Protection and Information Commissioner.

FIFA
Fédération Internationale de Football Association. For the purposes of these Regulations, the term "FIFA" includes any FIFA Subsidiary Company.

FIFA Subsidiary Company
Any legal person that belongs to FIFA or is under FIFA's control, whether wholly or partially (with FIFA holding a majority).

Member Association
Any national football association that has been admitted into membership of FIFA by the FIFA Congress.

Personal Data
Any information relating to a Data Subject.

Process / Processing / to process
Any 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.

Process Owner
Any person who is responsible for a Process in accordance with the hierarchical organisation of FIFA, the Member Associations or their members. If the Process Owner has not been and cannot be determined, the person responsible for the Entity Unit utilising the Process for its purpose or for facilitating its activities is considered to be the Process Owner.

Profiling
Any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.

Regulations
These FIFA Data Protection Regulations.

Special Categories of Personal Data
Any Personal Data revealing ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data or 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.

Third Party
Any natural or legal person, public body, agency or body other than an Entity or Data Subject, and persons who, under the direct authority of an Entity, are authorised to process Personal Data.

3 Scope

These Regulations apply to all activities of FIFA, without limitation.

These Regulations also apply to all Member Associations and all of their members. In this context, Member Associations are responsible for ensuring that they comply with these Regulations as well as for ensuring that their members comply with these Regulations. However, for Member Associations and their members, these Regulations are only applicable insofar as:

- they process Personal Data for, on behalf of, or with FIFA;
- they exchange or transfer Personal Data with FIFA, or with other Member Associations or their members, or with third parties on behalf of FIFA;
- they use infrastructure provided by FIFA to its Member Associations and their members for the purpose of Processing Personal Data.

These Regulations do not apply to Member Associations and their members in relation to any Personal Data that they cumulatively process:

- using their own infrastructure;
- for their own purposes; and
- in their own right.

4 Data Processing

1. Principles

FIFA processes Personal Data in compliance with the following principles. Personal Data must be:

- processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

Example: *The Processing of Personal Data can be considered lawful, fair and transparent when the name, surname, gender, date of birth and postal address are used to identify and send an event ticket to its purchaser, provided that the purchaser has been made aware of which Personal Data is being used and for what purpose.*

- collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further Processing for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes is considered to be compatible with the initial purposes;

Example: *If data for the purchase of an event ticket was collected for the sole purpose of issuing said ticket and the purchaser has not been made aware of the further usage of their Personal Data, that Personal Data may not be used for other purposes, i.e. resale to an official sponsor for marketing purposes.*

- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

Example: *Any Personal Data that is processed has to serve the purpose for which it has been collected. No additional Personal Data other than the data necessary to fulfil the intended purpose may be collected and further processed.*

- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that any Personal Data that is inaccurate, considering the purposes for which it is processed, is erased or rectified without delay;

Example: *All Personal Data has to be accurate. Data Subjects can request the correction of inaccurate Personal Data. Where possible and appropriate, the Process Owner can foresee means for the Data Subjects to access, examine and correct their Personal Data.*

- kept in a form that permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, subject to the implementation of the appropriate technical and organisational measures required by the Applicable Data Protection Laws in order to safeguard the rights and freedoms of the Data Subject;

Example: *The Process Owner is responsible for determining, together with other Entity Units if applicable, the maximum storage duration of Personal Data, and for documenting this decision.*

- processed in a manner that ensures the appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Example: *Appropriate organisational measures may include setting up internal Processes to comply with the Applicable Data Protection Laws, such as contractually binding volunteers, employees and contractors to the lawful Processing of data, issuing internal regulations, and carrying out awareness-raising and training exercises.*

- Personal Data is only accessible to people who need it for their activity ("need-to-know" principle);

Example: *Restrict access to HR data to the personnel handling data for human resources (HR Unit).*

- Every Entity shall ensure that all infrastructure used for the Processing of Personal Data is adequately protected with state-of-the-art and commercially reasonable technical and organisational measures, taking into consideration the risks that Data Subjects would encounter as a result of any non-compliant Processing of Personal Data.

2. Special Categories of Personal Data

Special Categories of Personal Data, e.g. data revealing ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation, shall be afforded special protection against unauthorised access.

All persons Processing Special Categories of Personal Data must be expressly advised of the importance of treating these Special Categories of Personal Data as strictly confidential.

Special Categories of Personal Data may only be transferred to Third Parties if there are legal reasons for doing so or with the express Consent of the Data Subject.

5 Data Subject's rights

The Data Subject has the following rights under the Applicable Data Protection Laws:

- the right to be informed about the collection and use of Personal Data;

Example: *Before any Personal Data is collected, the Data Subject must be informed about which Personal Data is being collected and for what purpose. The information needs to be easily or publically available, easy to access, and written in clear and simple language.*

- the right to access the Personal Data held about him. An access request must be fulfilled within 30 days. Data Subjects requesting access to their data must be able to identify themselves. The means of identification must be proportionate to the Personal Data to which the Data Subject is requesting access. Where feasible, technically appropriate and commercially reasonable, all Data Subjects should be able to access their data through a web interface that provides sufficient means of security and authentication;

Data Subjects have the right to ask which Personal Data the Entity in question is Processing and for what purposes. In order to be sure that the person placing the request really is the Data Subject he is claiming to be, means of authentication must be in place. Higher authentication measures are mandatory for access to sensitive data. Such measures may include a copy of an official identification document (government-issued ID, passport, driver's licence). In such a case, the transfer of such proof of identification also requires adequate protection. For access to low-sensitivity data from within a web application, the login credentials of the Data Subject are sufficient. In this case, it is recommended that the Data Subjects be granted access to their Personal Data from within the web application. As a general rule, access to Personal

Data from within a web application (e.g. a forum, a web shop with client credentials, etc.) can help to ease the Process of granting access.

- the right to rectification if any Personal Data held about him is inaccurate or incomplete;

Data Subjects are allowed to change their names, addresses, etc. or any other Personal Data if the existing data is inaccurate for any reason.

- the right to be forgotten – i.e. the right to ask that any Personal Data an Entity holds about him be deleted;

The means for Processing Personal Data must include tools to either irrevocably delete or anonymise Personal Data. Pseudonymous data is still considered to be Personal Data.

- the right to restrict (i.e. prevent) the Processing of Personal Data in accordance with the Applicable Data Protection Laws;

Should a Data Subject seek to make use of legal actions against an Entity, they can request that the use of their Personal Data be restricted until the lawfulness of its Processing is confirmed or denied.

- the right to data portability (obtaining a copy of the Personal Data to re-use with another service or organisation);

Data Subjects have the right to export a copy of their Personal Data in a machine-readable format. Should a web application foresee access to Personal Data, it may be appropriate to implement an export function for the accessed data within the access dashboard.

- the right to lodge a complaint with the competent supervisory authority and before the competent courts, in accordance with the Applicable Data Protection Laws;

- the right to obtain redress and, where appropriate, compensation for a breach of the Applicable Data Protection Laws; and

- where the Processing of Personal Data includes automated decision-making and Profiling, the right to request a human-based reassessment under the Applicable Data Protection Laws only when automated decision-making concludes in a decision that is legally binding upon the Data Subject.

6 Transmission of Personal Data to Third Parties/Data Processing by Third Parties

Personal Data may be transferred to a Third Party provided that the Processing is carried out in accordance with these Regulations and provided that no legal or contractual obligation to secrecy prohibits this practice. The transmission of Personal Data to Third Parties shall be carried out in such a way that the Third Party processes the data in accordance with the sender's instructions.

7 Cross-border Disclosure

1. Principles

Cross-border (i.e. outside Switzerland) Disclosure of Personal Data (including the granting of remote access) is permitted where the legislation in the country in question guarantees an adequate level of data protection according to the list published by the FDPIC.

2. Lack of an adequate level of data protection abroad

Personal Data may be disclosed cross-border to countries lacking an adequate level of protection if, alternatively:

a) these Regulations are complied with;
b) sufficient guarantees are agreed with the recipient in the form of a contract or in another legally enforceable form;
c) the Data Subjects grant their Consent on an exceptional basis;
d) the Processing of Personal Data is closely connected to the conclusion or performance of a contract and the data consists of the contractual partner's Personal Data;
e) it is required for the substantiation of claims before courts;
f) the Disclosure takes place within the same legal person or company, provided that the applicable internal data protection guidelines provide an appropriate level of protection.

8 Entity-internal Processing guidelines

1. Responsibilities
Every Entity is responsible for putting in place the necessary technical and organisational measures to guarantee compliance with these Regulations and the Applicable Data Protection Laws. The Entity shall ensure the training of its subordinates and their compliance with these Regulations. The Entity shall document the nature, purpose and grounds of the Processing it carries out, the technical and organisational measures put in place in order to comply with these Regulations, and any other relevant information with respect to the particular Processing.

2. Process Owner
Every Entity shall implement internal guidelines to identify a Process Owner for every Processing of Personal Data.

3. Data inventory
Each Entity shall keep an inventory of Processing activities. This inventory shall contain the following details:

- Name and contact information of the person responsible for the Processing
- Description of the Processing
- Purpose of the Processing
- Description of the categories of Data Subjects
- Description of the categories of Personal Data
- Special Categories of Personal Data
- Categories of recipients
- Identification of third countries (i.e. jurisdictions/international organisations outside Switzerland)
- Categories of recipients in third countries
- Safeguards in case of recipients in third countries
- Name of sub-processor
- Name/version of sub-processor agreement
- Data retention periods
- Technical and organisational security measures

4. Checks by the Process Owner
The Process Owner shall regularly check the information in the data inventory.

9 Information security requirements

All Personal Data must be protected against the risk of loss of confidentiality, integrity and availability. The Entity shall implement all necessary state-of-the-art and commercially reasonable organisational and technical measures. The Entity shall implement and enforce internal guidelines with respect to information security.

10 Data Security Incidents

Every event of loss of confidentiality, integrity and availability with the potential of constituting a risk for FIFA, another Entity or a Data Subject is to be treated as a Data Security Incident. Every Data Security Incident falling under the scope of these Regulations must be notified to alert@fifa.org.

Every Entity must ensure the constitution of a dedicated team taking action to eliminate Data Security Incidents. All Entities and Data Owners need to define clear procedures allowing for an immediate notification of a Data Security Incident internally and ultimately to FIFA. If another Entity is required to report a Data Security Incident to a competent authority under the Applicable Data Protection Laws under which it falls, FIFA shall also be notified accordingly.

11 Data Protection Officer (DPO)

FIFA has appointed a DPO. Data Subjects wishing to make use of any of their rights for Processing falling under the scope of these Regulations may contact the DPO by sending an email to dataprotection@fifa.org.

The DPO independently organises, analyses and monitors compliance with data protection provisions and in particular with these Regulations.

12 Final provisions

1. Official languages
If there are any discrepancies in the interpretation of the English, French, German or Spanish texts of these Regulations, the English text shall be authoritative.

2. Sanctions
Any infringement of these Regulations may incur sanctions under the Applicable Data Protection Laws, the FIFA Statutes or any other FIFA regulations.

3. Entry into force
These Regulations were approved by the FIFA Council on 24 October 2019 and come into force immediately.

Shanghai, 24 October 2019

For the FIFA Council:

President:
Gianni Infantino

Secretary General:
Fatma Samoura


MIX
Paper from
responsible sources
FSC® C006844
FSC
www.fsc.org

Fédération Internationale de Football Association