

DATA PROTECTION

WHAT?

The way we handle data is covered by different laws, both in Switzerland and across the world. For example, when it comes to data relating to individuals – also known as personal data – we are governed by the Swiss Federal Act on Data Protection and the European General Data Protection Regulation (GDPR). These laws aim to make sure that individuals' privacy is respected and their data is processed properly.

The FIFA Data Protection team supports FIFA to make sure we're all doing the right thing with data. They work closely with the divisions, offering training and advice to help team members protect personal data.

WHY?

Data protection is about trust – we want the people who interact with us to trust we'll do the right thing with their personal information. As well as loss of trust, there can be huge penalties for breaking the law: for example, fines for breaching GDPR can be up to €20 million.



WHO?

Data can come from anywhere: for example FIFA employees, players, referees, match officials, fans and stadium visitors. It's up to every team member who collects or processes personal data to understand their responsibilities and duties.

HOW?

FIFA has a number of teams with special responsibilities for data. The Data Protection Officer oversees data across the whole of FIFA and is the main point of contact for any external body with data protection queries. The Information Security Team helps keep our information safe and protected from attack, while the Incident Response Team provide a quick, effective, structured approach to data incidents including data breaches.

We follow all relevant laws for handling data and keep regular records of what we do and how we do it. We use data protection impact assessments to understand any potential risks or issues that might have an impact on individuals' privacy.

When it comes to third parties who process data for us, we work with FIFA Legal and Procurement to set up individual data processing agreements to make sure they understand their responsibilities.



FIFA - Data Protection
European Commission
Swiss Federal Data Protection and Information Commissioner
Annex I Definitions and examples

FIFA Compliance Pocket Guide

DATA PROTECTION

DATA PROTECTION IMPACT ASSESSMENT

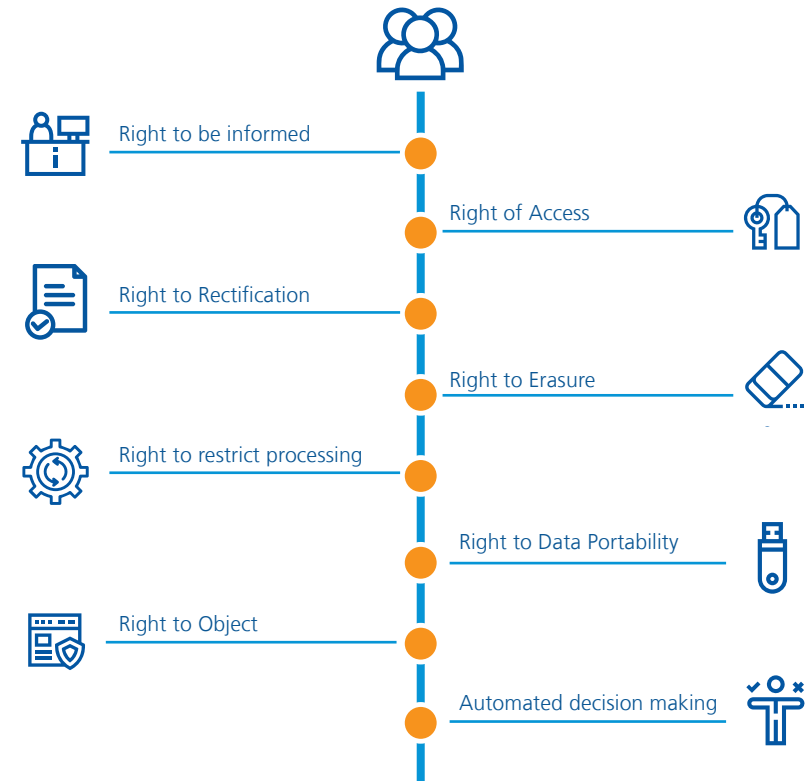
If you're kicking off a project which will involve processing personal data, FIFA's Data Protection team will help you perform a DPIA.



Our Data Protection Principles

- Data is processed lawfully, fairly and transparently
- Data is only collected for specific, legitimate purposes and not processed further in ways that don't meet the original purpose
- Data is kept accurate, up to date and only for as long as necessary
- We assure the confidentiality, integrity and availability of all personal data

RIGHTS OF DATA SUBJECTS UNDER THE GDPR



How do we handle data? We've set up a simple process to handle queries from individuals, simply by contacting dataprotection@fifa.org.

Do you know what to do? If individuals get in touch with you to ask about their data, forward the query to dataprotection@fifa.org. Or, if you're unsure of how to deal with a data protection query, contact FIFA's Data Protection team.

DATA PROTECTION

ANNEX I DEFINITIONS AND EXAMPLES

DATA PROTECTION IMPACT ASSESSMENT

Step 1: Description

Project teams tell us what data they want to use and why.

Step 2: Risks

FIFA's Data Protection Team assesses the data protection needed, assessing the risks and checking the proposed use of data is lawful.

Step 3: Measures

FIFA's Data Protection Team and the project team develop measures to manage any identified risks.

Step 4: Report

The final DPIA report documents risks, mitigations and implementation timings. The DPIA can be used internally and externally to show how we're doing the right things with data.

RIGHTS OF DATA SUBJECTS UNDER THE GDPR



Right to be informed: Before any personal data is collected, the individual must be informed about which personal data is being collected and for what lawful purposes. The information needs to be easily or publically available, easy to access, and written in clear and simple language. When using FIFA's websites, users need to be clearly informed by a data protection policy.



Right of Access: Individuals have the right to ask which personal data FIFA is processing on themselves and for what purposes. If a FIFA Team member wants to know which data FIFA holds about himself in a specific system the FIFA Data Protection Team (dataprotection@fifa.org) will provide that information as soon as possible.



Right to rectification: Individuals are allowed to change their names, addresses or any other personal data if the existing data is inaccurate for any reason. In case an employee changes his/her name after marriage, he/she can ask his/her HR Business Partner to change his/her surname in the system.



Right to erasure: Individuals must be provided with means to either irrevocably delete or anonymise personal data. A fan might ask his FIFA for his account to be deleted. In that case FIFA will either delete or alternatively anonymise the data for statistical reasons.



Right to restrict processing: Individuals may request that the use of their personal data to be restricted until the lawfulness of the particular processing is confirmed or denied. A new process to gather for example health data of players can be put "on hold" before a data protection impact assessment is performed.



Right to Data Portability: Individuals can obtain a copy of the personal data to re-use with another service or organisation in a machine-readable format. Should a web application foresee access to personal data, it is appropriate to implement an export function for the accessed data within the preference center.



Right to Object: In some cases individuals can object outright to having their personal data processed by an organisation. In case FIFA uses personal data for direct marketing purposes, FIFA would be obliged to immediately stop the processing for direct marketing purposes in case of objection by the data subject.



Right to object to automated decision making: An example of automated decision making would be using social media posts to analyse the personalities of fans by using an algorithm to analyse words and phrases which suggest "safe" and "unsafe" behaviour in order to assign seats at the stadium accordingly.