DATA PROTECTION

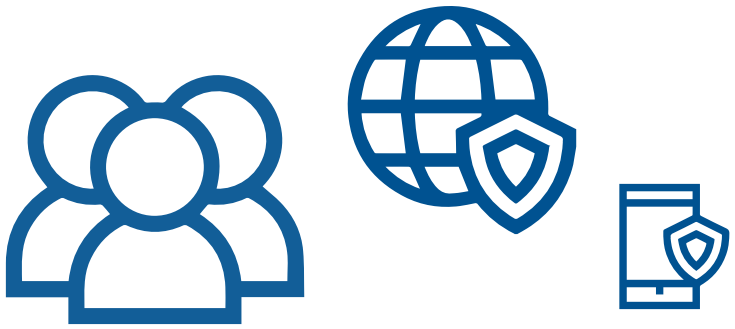
WHAT?

The way we handle data is covered by different laws, both in Switzerland and across the globe. 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 that 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 that we will 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 the GDPR can be over EUR 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 and structured approach to data incidents including data breaches.

We comply with all relevant legislation 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 FIFA Procurement to set up individual **data processing agreements** 🅘 to make sure that they understand their responsibilities.

FIFA – Data Protection
European Commission
Swiss Federal Data Protection and Information Commissioner
Annexe – Definitions and Examples

DATA PROTECTION

DATA PROTECTION IMPACT ASSESSMENT

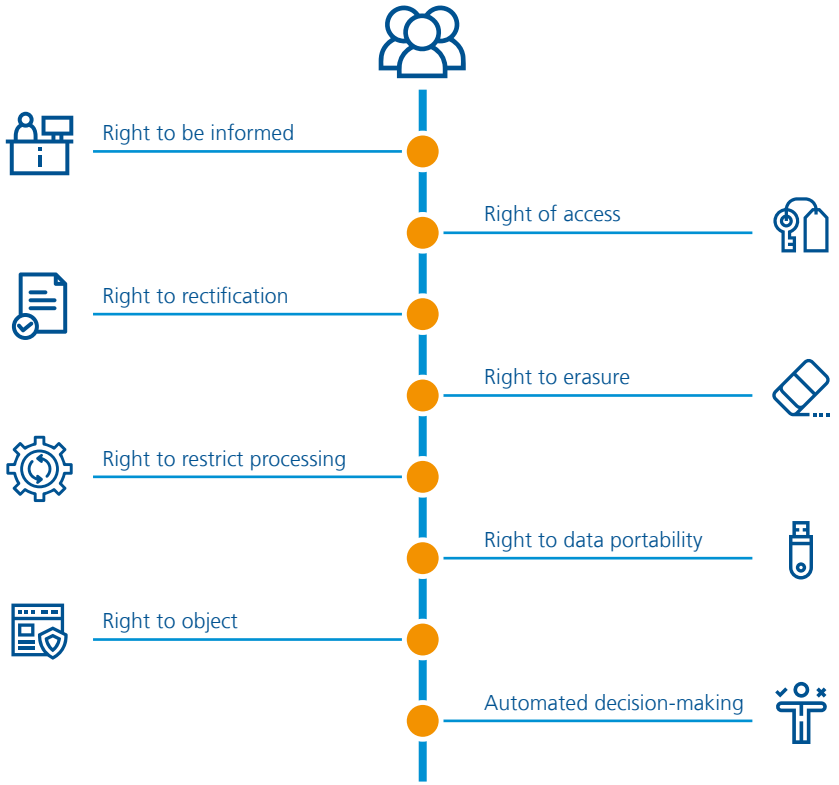
If you're kicking off a project that will involve processing personal data, FIFA's Data Protection team will help you perform a data protection impact assessment (DPIA).

DESCRIPTION → RISKS → MEASURES → REPORT

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 ensure 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, who simply have to contact 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.

ANNEXE: 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 degree of data protection needed, assessing the risks and checking that 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 both 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 on data matters 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 purpose. If a FIFA team member wants to know which data FIFA holds about him or her 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 name, address or any other personal data if the existing data is inaccurate for any reason. Employees who change their name after marriage can ask their HR Business Partner to make the change in the system.

Right to erasure: individuals may demand that their data be either irrevocably deleted or anonymised. For example, if a fan asks FIFA to delete his/her account, FIFA will either delete or, alternatively, anonymise the data.

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

Right to data portability: individuals have the right to obtain a copy of the personal data that FIFA keeps about them. This copy should be in a format that allows the individual to transfer the data to an alternative organisation. For example, a former FIFA employee can request FIFA to transfer his or her employee data to a new employer.

Right to object: in some cases, individuals can object outright to having their personal data processed by an organisation. If FIFA uses personal data for direct marketing purposes, it would be obliged to stop the processing for direct marketing purposes immediately in the event of an 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 examine words and phrases that suggest "safe" and "unsafe" behaviour in order to assign seats at the stadium accordingly.