Tavistock Football Development Centre Ltd

Youth Football Development Programme GDPR Policy

17 September 2024

1. Introduction

Tavistock Football Development Centre] ("we", "our", "us") is committed to protecting the privacy and security of personal data. This GDPR policy outlines how we collect, use, store, and protect personal information in compliance with the General Data Protection Regulation (GDPR).

2. Data Controller

For the purposes of the GDPR,TAvistock Football Development Centre is the data controller. Our contact details are:

Address: 18 Tamar Close, Bere Alston, PL207HF
Email: tavifootballdc@gmail.com
Phone: 07835756899

3. Data We Collect

We may collect and process the following categories of personal data:

Participant Information: Name, date of birth, gender, medical conditions, dietary requirements, emergency contact details, and parent/guardian information.
Contact Information: Email addresses, phone numbers, and postal addresses.
Attendance Records: Records of attendance at training sessions, matches, and events.
Media: Photographs and videos taken during training sessions, matches, and events.
Performance Data: Data related to player performance, assessments, and feedback.

4. Purpose of Data Processing

We collect and process personal data for the following purposes:

Programme Administration: To manage registrations, attendance, and participation in training sessions, matches, and events.
Communication. To inform participants and parents/guardians about schedules, changes, and other relevant information.
Health and Safety: To ensure the safety and well-being of all participants.
Development and Performance Monitoring: To track and evaluate player development and progress.
Promotional Activities: To use photographs and videos for promotional purposes on our website, social media, and other marketing materials (subject to consent).

5. Legal Basis for Processing

We rely on the following legal grounds for processing personal data:

Consent:For certain activities, such as using photographs and videos for promotional purposes, we will seek explicit consent from participants or their parents/guardians.
Contractual Necessity: To fulfill our obligations to participants as part of their registration and participation in the programme.
Legal Obligation: To comply with applicable laws and regulations.
Legitimate Interests:For purposes such as programme administration, communication, and development, where these interests are not overridden by individuals' rights.

6. Data Sharing

We may share personal data with third parties, including:

Coaches and Staff: To facilitate programme delivery and development.
Medical Professionals: In case of an emergency or medical necessity.
Governing Bodies: To comply with regulatory requirements or as required by the league or competition rules.
Service Providers: For IT support, data storage, or other necessary services.

We will never sell personal data to third parties.

7. Data Retention

We will retain personal data for as long as necessary to fulfill the purposes outlined in this policy, or as required by law. After this period, we will securely delete or anonymise personal data.

8. Data Security
We implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, or misuse. These measures include:

- Secure storage of physical records.
- Use of encrypted digital storage.
- Regular review and updating of data protection practices.

9. Rights of Data Subjects

Participants and their parents/guardians have the following rights concerning their personal data:

- Right to Access: To request access to personal data we hold.
- Right to Rectification: To request correction of any inaccuracies in personal data.
- Right to Erasure: To request deletion of personal data, subject to certain conditions.

If a breach occurs:

A GDPR (General Data Protection Regulation) breach refers to a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. When a GDPR breach occurs, organisations must follow a specific process to handle it appropriately and mitigate any potential damage. Here is an overview of the process:

1. Identify the Breach

The first step is to **identify** that a breach has occurred. A breach could involve:

- Loss of data (e.g., accidental deletion or loss of a device containing personal data).
- Unauthorised access (e.g., hacking, phishing attacks, or data sent to the wrong recipient).
- Data theft or disclosure(e.g., data shared without proper authorisation).

2. Contain the Breach

Once a breach is identified, the organisation must act quickly to **contain and limit** the breach. This may involve:

- Stopping any ongoing unauthorised access.
- Disabling affected systems or accounts.
- Retrieving or securing compromised data (e.g., recalling emails or disabling access to shared files).

3. Assess the Risk and Impact

After containing the breach, the organisation must assess the **risk and impact**. This involves understanding:

What personal data was affected: What type of data was involved (e.g., sensitive data, financial information, contact details).
- Whose data was affected: The number of individuals impacted and the potential consequences for them.
- Potential harm to individuals:The risk of financial loss, identity theft, reputational damage, discrimination, or other significant impact on data subjects.

4. Report the Breach (If Necessary)

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it must be reported:

-To the Supervisory Authority: The organisation must notify the relevant Data Protection Authority (DPA) within 72 hours of becoming aware of the breach, if possible. The notification should include:
  - A description of the nature of the breach, including the categories and approximate number of data subjects and personal data records affected.
  - The name and contact details of the Data Protection Officer (DPO) or other contact point.
  - The likely consequences of the breach.
  - Measures taken or proposed to be taken to address the breach and mitigate its effects.

- **To the Affected Individuals:** If the breach poses a **high risk** to the rights and freedoms of individuals, the organisation must also notify the affected individuals **without undue delay**. The notification should be in clear and plain language and include:
  - A description of the breach and its likely impact.
  - Contact details of the DPO or relevant contact point.
  - Recommendations for individuals to mitigate potential adverse effects (e.g., changing passwords, monitoring accounts).

5. Investigate the Breach

The organisation should conduct a thorough investigation to understand:

- The **root cause** of the breach.
- The effectiveness of the response and containment measures.
- Any weaknesses or vulnerabilities that need to be addressed.

This investigation should also aim to identify any compliance gaps and consider improvements to policies, procedures, and technical measures.

6. Take Remedial Action

Based on the findings of the investigation, the organisation should take appropriate steps to:

- Rectify any data security weaknesses or vulnerabilities.
- Implement additional safeguards to prevent future breaches (e.g., improved encryption, more robust access controls, staff training).
- Document the incident, its impact, and the steps taken to mitigate it. Maintaining detailed records of breaches is essential for demonstrating compliance with GDPR obligations.

7. Review and Update Policies and Procedures

Following a breach, it is vital to review and, if necessary, update the organisation's:

- Data protection policies and procedures to reflect lessons learned.
- Incident response plan to improve the handling of future breaches.
- Training programs to raise awareness among staff and reduce the risk of human error.

8. Maintain a Data Breach Register

Under GDPR, organisations must maintain a **data breach register** to record all breaches, regardless of whether they need to be reported to the supervisory authority. This register should include:

- Details of the breach (what happened and when).
- The nature and volume of the data involved.
- The response and actions taken.
- Any communications with the supervisory authority and affected individuals.

Key Takeaways

- Act quickly to identify, contain, and assess the breach.
- Report the breach to the appropriate supervisory authority and affected individuals if it poses a high risk.
- Investigate, document, and learn from the breach to strengthen data protection measures.
- Maintain a breach register to document all breaches, reported or otherwise.

By following these steps, an organisation ensures compliance with GDPR and minimises the impact of any data breaches on individuals and the organisation.