

DATA PROTECTION POLICY

1. Purpose

This Data Protection Policy (“Policy”) sets out the principles and practices that International Football Sports Group (IFSG) follows to ensure that personal data is collected, processed, stored, and disposed of in a lawful, fair, and transparent manner.

IFSG is committed to protecting the privacy and rights of individuals whose personal data we process, and to complying with all applicable data protection and privacy laws, including the General Data Protection Regulation (GDPR) (where applicable), national data protection legislation, and relevant international standards.

2. Scope

This Policy applies to:

- All employees, officers, directors, contractors, consultants, and temporary staff of IFSG.
- All third parties, suppliers, and partners who process personal data on behalf of IFSG.
- All business operations, systems, and processes involving the collection, storage, processing, transfer, or disposal of personal data.

This Policy covers all personal data processed by IFSG in any format — electronic, paper, or otherwise.

3. Definitions

Personal Data: Any information relating to an identified or identifiable individual, such as name, contact details, identification numbers, location data, or online identifiers.

Special Category Data: Sensitive personal data including racial or ethnic origin, political opinions, religious beliefs, health information, biometric data, or data concerning a person’s sex life or sexual orientation.

Processing: Any operation performed on personal data, including collection, recording, storage, use, disclosure, or deletion.

Data Subject: The individual to whom the personal data relates.

Data Controller: The entity that determines the purposes and means of processing personal data.

Data Processor: A third party that processes personal data on behalf of the controller.

4. Policy Statement

IFSG is committed to ensuring that all personal data is:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

- Accurate and kept up to date, with every reasonable step taken to ensure that inaccurate data is corrected or deleted without delay.
- Stored no longer than necessary for the purposes for which it is processed.
- Processed securely using appropriate technical and organizational measures to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage.

5. Legal Bases for Processing

IFSG will process personal data only where at least one of the following lawful bases applies:

- The data subject has given explicit consent.
- Processing is necessary for the performance of a contract.
- Processing is required for compliance with a legal obligation.
- Processing is necessary to protect vital interests of the data subject or another person.
- Processing is necessary for the performance of a task carried out in the public interest.
- Processing is necessary for the legitimate interests pursued by IFSG or a third party, provided such interests are not overridden by the rights and freedoms of the data subject.

6. Data Subject Rights

IFSG respects the rights of individuals and will respond promptly and appropriately to requests to exercise those rights, which include:

- Right to be informed – about how their data is processed.
- Right of access – to obtain a copy of their personal data.
- Right to rectification – to correct inaccurate or incomplete data.
- Right to erasure (“right to be forgotten”) – under certain circumstances.
- Right to restrict processing – in certain situations.
- Right to data portability – to receive personal data in a structured, commonly used format.
- Right to object – to certain types of processing.
- Rights related to automated decision-making – including profiling.

All such requests must be directed to the Data Protection Officer (DPO) and handled in accordance with applicable legal timeframes.

7. Data Security

IFSG implements appropriate technical and organisational measures to protect personal data, including but not limited to:

- Access controls and authentication mechanisms.
- Data encryption and secure storage.
- Regular security assessments and audits.
- Policies governing the use of devices, passwords, and remote access.
- Staff training on data protection and cybersecurity best practices.

Any actual or suspected data breach must be reported immediately to the DPO. IFSG will investigate all incidents promptly and, where required, notify regulatory authorities and affected individuals.

8. Data Sharing and Third Parties

Personal data will only be shared with third parties where:

- It is necessary for legitimate business purposes.
- The third party provides sufficient guarantees of implementing appropriate data protection measures.
- A written data processing agreement is in place, outlining the responsibilities of both parties.

International data transfers will only occur where adequate safeguards are in place, such as Standard Contractual Clauses, Binding Corporate Rules, or transfers to jurisdictions deemed adequate by relevant authorities.

9. Data Retention and Disposal

Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected, including legal, accounting, or reporting obligations.

Once data is no longer required, it will be securely deleted, anonymized, or destroyed in accordance with IFSG's Data Retention and Disposal Policy.

10. Roles and Responsibilities

Board of Directors: Overall accountability for data protection compliance.

Data Protection Officer (DPO): Oversight of data protection activities, compliance monitoring, handling of data subject requests, and liaison with supervisory authorities.

Managers: Ensuring team compliance with this Policy and related procedures.

All Staff: Understanding and following this Policy, reporting data breaches, and protecting personal data within their control.

11. Training and Awareness

All employees and relevant third parties must complete mandatory data protection training and regular refresher sessions. Training ensures awareness of legal obligations, best practices, and IFSG's policies and procedures.

12. Breach Management

All actual or suspected data breaches must be reported immediately to the DPO.

IFSG will:

- Investigate the incident promptly.
- Mitigate potential risks and impacts.
- Notify supervisory authorities and affected individuals where legally required.
- Document all breaches and lessons learned to prevent recurrence.

13. Policy Review

This Policy will be reviewed annually or sooner if required by changes in legislation, business operations, or best practices. Updates will be communicated to all staff and relevant stakeholders.

Approved by: ROBERT SMETHURST

Title: OWNER & DIRECTOR

Date: January 2024