Data Protection and Privacy

February 2023

Helping community groups survive,
to help young people thrive.

+44 (0) 203 848 4670
info@sported.org.uk

Registered office: Sported Foundation, 190 Great Dover Street, London SE1 4YB

Registered Charity Numbers: 1123313 | SCO43161
Company No: 06541137

Data Protection and Privacy

Introduction and Purpose

Sported needs to collect and use certain information about individuals, known as Data Subjects, in order to run its business effectively.

The General Data Protection Regulation ("GDPR") 2018 was introduced an updated personal data privacy law across all EU member states and replaces the Data Protection Directive 95/46/EC. GDPR governs the processing, such as the use or holding, of personal data, which is essentially any information about identifiable living individuals, and also gives those individuals certain rights and remedies in respect of that information.

Sported is defined as a Data Controller under GDPR since it determines the purposes for which, and the manner in which, any personal data on Data Subjects are to be processed. Sported must comply with seven principles regarding personal information under GDPR. Furthermore, Sported must notify the Information Commissioner's Office ("ICO") of certain details about its processing of personal information.

The misuse or unregistered use of personal data by Sported or its employees can result in criminal prosecution and claims for compensation.

As the UK Supervisory Authority, the ICO can implement fines against firms found to have breached GDPR which depending on the seriousness, duration, and nature of infringement can be severe. A two-tiered sanction regime is applied:

- Up to €20 Million or 4% of global annual turnover for the preceding financial year, whichever is the greater
- Up to €10 Million or 2% of global turnover, whichever is greater.

Additionally, if a data subject's rights are breached they are able to sue an organisation for material or non-material damages as an individual or as part of class action. There is no upper limit set by GDPR for these damages and the action may be brought about in either the firm or data subjects country.

DEFINITIONS

Personal data is data that relates to a living individual who can be identified either from that data, or from other information which is in the possession of (or is likely to come into the possession of) the Data Controller i.e. Sported. Personal data includes financial information, any expression of opinion, or indication of intentions, held by us regarding the individual.

Sensitive data means data pertaining to: racial or ethnic origin; religious or similar beliefs; trade union membership; physical or mental health or sexual life; political opinions; criminal offences. This data may only be held in strictly defined situations or where explicit consent has been obtained.

A Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed. A data controller must be a "person" recognised in law, that is to say:

- individuals;
- organisations; or
- other corporate and unincorporated bodies of persons.

In relation to data controllers, the term "jointly" is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term "in common" applies where two or more persons share a pool of personal data that they process independently of each other.

Data processing of personal information or data, means obtaining, recording or holding the information or data; or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data,
- Retrieval, consultation or use of the information or data,
- Disclosure of the information or data by transmission, dissemination or otherwise making available, or

+44 (0) 203 848 4670
info@sported.org.uk

Registered office: Sported Foundation, 190 Great Dover Street, London SE1 4YB

Registered Charity Numbers: 1123313 | SCO43161
Company No: 06541137

- Alignment, combination, blocking, erasure or destruction of the information or data.

The definition of processing is broad and as such it is difficult to think of anything an organisation might do with data that will not be processing.

APPLICABILITY

This policy affects everyone employed by Sported since individuals who knowingly breach the GDPR can be held personally (and potentially criminally) liable.

POLICY

Everyone who is responsible for controlling and processing personal data at Sported must follow the strict rules set out within the 7 key the principles which guide GDPR:

- **Legality** – Data is processed lawfully, transparently and fairly
- **Purpose Limitation** – Data should be collected for a specified legitimate and explicit purpose
- **Minimisation** – Only Data that is relevant, adequate and necessary is collected
- **Accuracy** - Data is always up to date and inaccurate data is erased or rectified without delay
- **Storage Limitation** - Data is retained for no longer than is necessary
- **Integrity and Confidentiality** – Data shall be processed in a manner that ensures appropriate security against unauthorised or unlawful loss, destruction or damage
- **Accountability** - Ensuring robust processes and documentation is in place to handle data

PROCEDURE

Sported will implement the following procedures to comply with GDPR.

Helping community groups survive, to help young people thrive.

+44 (0) 203 848 4670
info@sported.org.uk

Registered office: Sported Foundation, 190 Great Dover Street, London SE1 4YB

Registered Charity Numbers: 1123313 | SCO43161
Company No: 06541137

REGISTRATION WITH ICO

Sported as a data controller who may process personal information in the course of its business has registered with the ICO and will renew its registration annually. See http://ico.org.uk/for_organisations/data_protection/registration for details.

DATA PROTECTION LEAD/OFFICER

Sported has appointed a Data Protection Lead/Officer at a senior level with specific responsibility for day today matters of data protection and acts as a contact point with the ICO.

The Data Protection Officer will act as a central point of reference for Sported on all issues relating to data protection and should be consulted in relation to all Data Protection Impact Assessments and Data Breaches.

The Data Protection Officer will monitor Sported's compliance with GDPR which includes the assignment of responsibilities, awareness raising, training and audits.

DATA PROTECTION IMPACT ASSESSMENTS

Under GDPR, Data Protection Impact Assessment's (DPIA) are an essential compliance tool which are primarily aimed at identifying risks relating to personal data. It is mandatory that a DPIA is undertaken when designing or modifying a process that involves the processing of personal information. Examples of areas where a DPIA must be carried out are:

- Changes to customer KYC and suitability checks
- Changes to marketing processes
- Changes to storage procedures or systems
- Changes to internal HR administrative procedures

Sported view DPIA' as vital in not only identifying risk to personal information but also a key tool in preventing unlawful processing and data breaches. At least annually the Data Protection Officer will carry out a review of the Sported DPIA's and report any key findings to the board. This is carried out as part of the risk register review every quarter.

+44 (0) 203 848 4670
info@sported.org.uk

Registered office: Sported Foundation, 190 Great Dover Street, London SE1 4YB

Registered Charity Numbers: 1123313 | SCO43161
Company No: 06541137

LAWFUL PROCESSING AND CONSENT

For processing to be lawful under GDPR, Sported need to identify a lawful basis before it is able to process personal data and it is vitally important that documentation is held to support this. There are 4 key areas which Sported rely on in lawfully processing personal data:

- Processing takes place with the explicit consent of the Data Subject
- Processing is necessary for the performance of a contract or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary for the purpose of legitimate interests of Sported expect where such interests are overridden by the interest, rights, or freedoms of the data subject.

CONSENT

Where Sported is processing data with consent then this must be a freely given, specific, informed and unambiguous indication of the data subjects wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and organisation will need to provide simple ways for people to withdraw consent.

Where Sported relies on individuals' consent to process their data, the firm will make sure that this meets the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn and that this consent is appropriately documented

LEGITIMATE INTEREST

In instances where Sported is processing data based on its legitimate interests this must only be carried out following the completion of a Legitimate Interest Assessment ("LIA") and is authorised by the Data Protection Officer.

The LIA is a balance test which assesses whether the legitimate interests of Sported outweigh the rights and freedoms of the data subject. The LIA must address the clear need to satisfy Sported's legitimate interest and show that the there is no other way to meet this. The LIA will then need to display that Sported needs outweighs the rights of the data subject and that the processing is both fair and lawful.

DATA COLLECTION

When collecting personal data Sported must always make sure that the Data Subjects knows:

- Who Sported is
- What the data will be used for
- To whom it will be disclosed.

This information should be provided on an application form or similar in order to ensure that the person is aware and consents to the processing of their personal data. If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place. It is important not to collect more personal data than is actually needed.

HANDLING DATA

When handling, collecting, processing or storing personal data employees must ensure that:

- All personal data is both accurate and up to date
- Errors are corrected effectively and promptly
- That the Sported data retention policy is adhered to. Data will be deleted/destroyed when it is no longer needed
- Personal data is kept secure at all times (see Data Security Policy)
- Written contracts are used when external bodies process/handle the data explicitly specifying the above requirements with respect to the data.

Employees must NOT:

- Access personal data that they do not require for their work;
- Use the data for any purpose it was not explicitly obtained for;
- Keep data that would embarrass or damage Sported if disclosed (via a subject access request – see below);
- Store/process/handle sensitive personal data unless the employee is certain Sported is entitled to or consent from the individual concerned has been obtained.

SUBJECT ACCESS REQUESTS

Under GDPR a key right of data subjects is that of being able to learn and have access to what personal information is held on them and by whom. This is known as a subject access request.

When a subject access request is received Information must be provided without delay and at the latest within one month of receipt. Sported may extend the period of compliance by a further two months where requests are complex or numerous. In such instances Sported must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

When Sported receives a subject access request the firm will provide a copy of the information held free of charge. Sported may charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that Sported will charge for all subsequent access requests rather that the firm reserves the right to charge a fee based on the administrative cost of providing the information.

If after reviewing a request the Data Protection Officer believes a request is manifestly unfounded or excessive, particularly if it is repetitive, then Sported may charge a 'reasonable fee' which will be decided on a case by case basis. In certain circumstances Sported may even refuse to respond to such requests.

Where Sported refuses to respond to a request, it must explain clearly to the individual why this is the case, informing them of their right to complain to the ICO and to a judicial remedy without undue delay and at the latest within one month.

PROVIDING THE INFORMATION

Before responding to a subject access request the identity of the person making the request must be verified.

If the request is made electronically, Sported will look to provide the information in a commonly used electronic format.

REQUESTS FOR LARGE AMOUNTS OF PERSONAL DATA

Where a subject access requests requires Sported to process a large quantity of information about an individual, GDPR permits the firm to ask the individual to specify the information to which the request relates. The GDPR does not include an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

WITHHOLDING INFORMATION

Sported is allowed to withhold information when it relates to the prevention, detection or investigation of financial crime. In such instances Sported doesn't have to say why it is withholding information. Where there is any doubt as to whether the supply of information to a data subject may breach the 'tipping off' obligations, then the Data Protection Officer/MLRO should be consulted, who may in turn may contact the National Crime Agency (NCA) for guidance.

DATA BREACHES

A personal data breach is defined as a breach of security which leads to the destruction, loss, alteration, unauthorised destruction of, or access to personal data. A breach therefore means more than just losing personal data.

Sported has a duty to notify the ICO of a breach where it is likely result in a risk to the rights and freedoms of an individual. Such a breach, if unaddressed, may

have a significant detrimental effect on an individual such as resulting in discrimination, damage to reputation and a loss of confidentiality.

Where a breach is likely to result in a high risk to the rights and freedoms of a data subject they must be notified directly. High risk therefore means that the threshold for notifying an individual is set higher than for when organisation must notify the relevant supervisory authority.

A notifiable data breach must be reported to the ICO within 72 hours of the organisation becoming aware of it. Failing to notify a breach can result in a fine of up to 10 million Euros or 2 percent of a firm's global turnover.

Should you suspect that a data breach has occurred you should notify your DPO or Compliance Officer immediately. Further details can be found in the Sported data security policy.

COMPLAINTS

If there are any concerns about our use of personal information, a complaint can be made to us using the contact details below in the footer.

A complaint can also be made to the ICO if anyone is unhappy with how we have used data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk