Data Protection Policy

10 May 2018

Version 1.2

Contents

1. Introduction

1.1 **scottish**athletics needs to gather and use certain information about individuals. These can include members, customers, suppliers, business contacts, volunteers, partners, employees, workers and other people the organisation has a relationship with or may need to contact.

1.2 This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards, and to comply with the law.

2. Purpose of this Policy

2.1 This Data Protection Policy ensures **scottish**athletics:

(a) Complies with data protection laws and follows good practice;
(b) Protects the rights of members, customers, suppliers, business contacts, volunteers, partners, employees and workers;
(c) Is open about how it stores and processes individuals' data; and
(d) Protects itself from the risks of a data breach.

3. Policy Objectives

3.1 The Data Protection Legislation requires **scottish**athletics, as a controller (the person who determines the purposes and means of processing any personal data in its possession), to handle personal data held in electronic files and within highly structured paper files in a responsible manner. The Data Protection Legislation applies to all activities undertaken by **scottish**athletics in relation to personal data and applies to the processing of personal data relating to data subjects by controllers.

3.2 Another body which is subject to the Data Protection Legislation is a processor, who processes personal data on behalf of a controller, for example, where membership administration is outsourced to a third party, that third party will usually be a processor of any personal data that it processes in providing that function to **scottish**athletics. Processors also have obligations under the Data Protection Legislation.

3.3 Data is information that is held on a computer, any electronic device, including smart mobile phones, and within highly structured paper filing systems. Such paper filing systems are those that are set up in a way that particular information in relation to a specific individual is readily accessible according to specific criteria.

3.4 For data to be personal, it has to relate to an identified or identifiable living individual. This also includes pseudonymised data, which could identify an individual if additional information is used.

3.5 The Data Protection Legislation contains additional rules in relation to the processing of special categories of personal data, which consists of data relating to an individual's:

(a) Racial or ethnic origin;
(b) Political opinions;
(c) Health;
(d) Sexual life or sexual orientation;

(e) Religious or philosophical beliefs;
(f) Trade union membership; and
(g) Genetic/biometric data for the purpose of uniquely identifying an individual.

3.6 The Data Protection Legislation expressly prohibits the processing of special categories of personal data, unless specific conditions apply. **scottish**athletics must meet a legal basis and at least one special condition before processing any special category of personal data.

3.7 Processing of personal data covers any activity carried out by **scottish**athletics on personal data, including collecting, storing, using, disclosing, amending and deleting.

3.8 **scottish**athletics must comply with the six data protection principles (the "DPPs") contained within the Data Protection Legislation when handling personal data. The DPPs apply during the full lifecycle of personal data within **scottish**athletics, from its collection to its continued use and through to its ultimate deletion.

3.9 As controllers, **scottish**athletics must comply with the DPPs. The DPPs require **scottish**athletics ensure that:

(a) Personal data is processed lawfully, fairly and in a transparent manner;
(b) Personal data is collected only for specified, explicit and legitimate purposes and not processed in a manner which is incompatible with those purposes;
(c) Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
(d) Personal data is accurate and, where necessary, kept up to date, every reasonable step taken to erase or rectify personal data which is inaccurate;
(e) Personal data is not kept for longer than is necessary; and
(f) Personal data is processed in a manner that ensures appropriate security of personal data, including protection against using unauthorised or unlawful processing, accidental loss of or destruction or damage to personal data.

4. Policy Statement

4.1 Our Data Protection Policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

4.2 We are committed to:

(a) Ensuring that we comply with the six data protection principles, as listed above;
(b) Meeting our legal obligations as laid down by the Data Protection Legislation;
(c) Establishing appropriate retention periods for personal data through our Data Retention Policy;
(d) Ensuring that data subjects' rights can be appropriately exercised;
(e) Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues;
(f) Ensuring that all employees, workers, volunteers and people working on behalf of **scottish**athletics are made aware of good practice in data protection;
(g) Providing adequate training for all those responsible for personal data;
(h) Ensuring that everyone handling personal data knows where to find further guidance;
(i) Ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly; and
(j) Regularly reviewing data protection procedures and guidelines within the organisation.

5. Scope of the Policy

5.1 This policy applies to:

(a) All premises that **scottish**athletics operates from;
(b) All employees, workers and volunteers of **scottish**athletics;
(c) All contractors, suppliers and other people working on behalf of **scottish**athletics.

5.2 It applies to all data that the company holds relating to identifiable individuals. This can include:

(a) Names of individuals;
(b) Contact details;
(c) Athlete performance data;
(d) Education and training records;
(e) Membership records; and
(f) Any other information relating to individuals.

6. Data Protection Risks

6.1 This policy helps to protect **scottish**athletics from some very real data security risks, including:

(a) Breaches of confidentiality - information being given out inappropriately;
(b) Failing to offer choice - all individuals should be free to choose how the company uses data relating to them; and
(c) Reputational damage - the company could suffer if hackers successfully gained access to sensitive data.

7. Responsibilities

7.1 Everyone who works for or with **scottish**athletics has some responsibility for ensuring data is collected, stored and handled appropriately.

7.2 Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

7.3 However, these people have key areas of responsibility:

7.4 Board

7.4.1 The Board is ultimately responsible for ensuring that **scottish**athletics meets its legal obligations.

7.5 Head of Operations

7.5.1 The Head of Operations is responsible for:

(a) Keeping the Board updated about data protection responsibilities, risks and issues;
(b) Reviewing all data protection procedures and related policies;
(c) Ensuring data protection training and advice for the people covered by this policy, is provided;
(d) Handling data protection questions from anyone covered by this policy;

(e) Dealing with requests from individuals to see the data **scottish**athletics holds about them (also called 'subject access requests');
(f) Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.;
(g) Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
(h) Evaluating any third-party services the company is considering using to store or process data; and
(i) Approving any data protection statements attached to communications such as emails and letters.

7.6 Head of Communications

7.6.1 The Head of Communications is responsible for:

(a) Addressing any data protection queries from journalists or media outlets such as newspapers; and
(b) Where necessary, working with others to ensure marketing initiatives abide by data protection principles.

8. General Guidelines

(a) The only people able to access data covered by this policy should be those who need it for their work.
(b) Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
(c) **scottish**athletics will provide training to all employees to help them understand their responsibilities when handling data.
(d) Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
(e) In particular, strong passwords must be used and they should never be shared.
(f) Personal data should not be disclosed to unauthorised people, either within the company or externally.
(g) Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of and in line with the Data Retention Policy guidelines.
(h) Employees should request help from their line manager or the Head of Operations if they are unsure about any aspect of data protection.

9. Data storage

9.1 These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Head of Operations.

9.2 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

9.3 These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

(a) When not required, the paper or files should be kept in a locked drawer or filing cabinet;
(b) Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer; and
(c) Data printouts should be shredded and disposed of securely when no longer required.

9.4 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

(a) Data should be protected by strong passwords that are changed regularly and never shared between employees, workers, volunteers, contractors, suppliers and other people working on behalf of **scottish**athletics;
(b) If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used;
(c) Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services;
(d) Servers containing personal data should be sited in a secure location, away from general office space;
(e) Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures;
(f) Data should never be saved directly to laptops or other mobile devices like tablets or smart phones; and
(g) All servers and computers containing data should be protected by approved security software and a firewall.

10. Data Use

10.1 Personal data is of no value to **scottish**athletics unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

(a) When working with personal data, employees, workers, volunteers, contractors, suppliers and other people working on behalf of **scottish**athletics should ensure the screens of their computers are always locked when left unattended;
(b) Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure;
(c) Data must be encrypted before being transferred electronically. The Head of Operations can explain how to send data to authorised external contacts;
(d) Personal data should never be transferred outside of the European Economic Area; and
(e) Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

11. Data Accuracy

11.1 The law requires **scottish**athletics to take reasonable steps to ensure data is kept accurate and up to date.

11.2 It is the responsibility of all employees, workers, volunteers, contractors, suppliers and other people working on behalf of **scottish**athletics, and who work with data, to take reasonable steps to ensure it is kept as accurate and up to date as possible.

(a) Data will be held in as few places as necessary. Any unnecessary additional data sets should not be created;
(b) All employees, workers, volunteers, contractors, suppliers and other people working on behalf of **scottish**athletics, should take every opportunity to ensure data is updated. For instance, by confirming a member's details when they call;
(c) **scottish**athletics will make it easy for data subjects to update the information **scottish**athletics holds about them. For instance, via the company website; and
(d) Data should be updated as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

12. Subject Access Requests

12.1 All individuals who are the subject of personal data held by **scottish**athletics are entitled to:

(a) Ask what information the company holds about them and why;
(b) Ask how to gain access to it;
(c) Be informed how to keep it up to date; and
(d) Be informed how the company is meeting its data protection obligations.

12.2 The Data Protection Legislation provides that, in order to meet these obligations, a copy of the personal data in electronic form, where the request is made by electronic means, must be provided unless otherwise requested by an individual.

12.3 A subject access request must:

(a) Be addressed in writing to **scottish**athletics (including email);
(b) Contain information to enable **scottish**athletics to satisfy itself as to the identity of the individual making the request; and provide information to enable **scottish**athletics to locate the personal data sought.

12.4 **scottish**athletics must comply with requests promptly and, in any event, within one month from the receipt of the request or from the receipt of the information necessary to enable **scottish**athletics to comply with the request (for example, from the date of the provision of sufficient information to allow for the verification of the identity of the data subject), whichever is later. It is possible to extend this time period by two months but only for complex or numerous subject access requests.

12.5 Where disclosure in response to a subject access request includes the disclosure of third party personal data to the individual making the request, such as the personal data of witnesses on the field of play or in a disciplinary context, then the Data Protection Legislation provides that, if it is not possible to edit or delete the third party data, **scottish**athletics need not provide information in response to a subject access request unless the third party concerned has consented or it is reasonable in all the circumstances to comply with the subject access request without such consent.

12.6 Subject access requests from individuals should be made by email to dataprotection@scottishathletics.org.uk. **scottish**athletics will aim to provide the relevant data within 15 working days, and **scottish**athletics will always verify the identity of anyone making a subject access request before handing over any information.

13. Disclosing Data for Other Reasons

13.1 In certain circumstances, the Data Protection Legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

13.2 Under these circumstances, **scottish**athletics will disclose requested data having ensured that the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary. For any welfare related issues, the Welfare Officer will do the same.

14. Providing information

14.1 **scottish**athletics aims to ensure that individuals are aware that their data is being processed, and that they understand:

(a) How the data is being used; and
(b) How to exercise their rights.

15. Data Breaches

15.1 Any breach of data protection must be reported immediately to the Head of Operations, or in their absence the Chief Executive Officer. Breaches are loss or damage, or potential loss or damage, to data and include such circumstances as loss or damage to a computer or smartphone.

To these ends, **scottish**athletics has a privacy notice, setting out how data relating to individuals is used by the company. This is available on the **scottish**athletics website at https://www.scottishathletics.org.uk/about/privacy-notices

scottishathletics Board

10/05/2018

Equality Impact Assessment Record

Date of Assessment:	10 May 2018
Assessed by:	Head of Operations, Equalities Officer.
Review date:	10/05/2021 or as legislation dictates, whichever is first.