****

**Governance Code for Sport**

**Data Protection Guidelines**

Guidance Notes and Checklist

Disclaimer

Sport Ireland is making available a range of resources including guidance notes, policy documents and templates for selected areas aligned to the Governance Code for Sport which will support sport organisations, boards, management and staff in the development of relevant governance processes and procedures particular to their own organisation.

For the avoidance of doubt, the final decision on the nature, type, extent and format of approved governance policies, procedures and processes for each organisation is a matter for the board / highest governing structure of the organisation and the resources and material provided may assist the approval process.

This document is not, nor is it intended to be, a definitive statement of the law and it does not constitute legal advice.

This document is not a substitute for professional advice from an appropriately qualified source and it is recommended that sport organisations consult their governing document or obtain their own independent legal advice where necessary. Sport Ireland does not accept any responsibility or liability for any errors, inaccuracies or omissions in this document.

**Why an organisation needs data protection guidelines**

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas, and came into effect in May 2018. The Data Protection Act 2018 is the relevant Irish legislation.

Principle 2 of the Governance Code for Sport (the Code) is about ‘Exercising Control over the Organisation’ specifically ‘Identifying and complying with all relevant legal and regulatory requirements’.  All organisations, whether Type A, B or C are obliged to comply with GDPR regulations. Putting in place and enforcing data protection guidelines will ensure that organisations are meeting their obligations under GDPR legislation.

In simple terms, GDPR sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). GDPR legislation essentially asks that personal data be processed under the following six principles:

1) Lawfulness, fairness and transparency

2) Purpose limitation

3) Data minimisation

4) Accuracy

5) Storage limitation

6) Integrity and confidentiality

An organisation must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. An organisation must take responsibility for their processing of personal data and how they comply with the GDPR, and be able to demonstrate (through appropriate records and measures) their compliance

An organisation’s data protection guidelines should ensure that any personal data held by the organisation is processed according to the above principles.

Whose responsibility is it to develop data protection guidelines?

It is the responsibility of the Board to ensure that all the principles of the Code are being upheld and delivered. The executive lead / Chief Executive Officer (CEO) is likely to be tasked with ensuring that the principles of the Code are being implemented in the organisation and thus will be responsible for ensuring data protection guidelines are in place and being used internally. In an organisation with an IT Manager, the guidelines may be within their remit. In a volunteer led organisation there may be a volunteer with specific expertise in the area who will write the policy/guidelines. Under the GDPR, certain organisations are required to appoint a designated Data Protection Officer (DPO), whose responsibility it will be to ensure data protection guidelines are being followed. Certain organisations are also required to publish the details of their DPO and provide these details to their national supervisory authority (in this case the Data Protection Commission).

What is GDPR and data protection?

Processing of personal data includes the following: collecting, recording, storing, adapting, using, disclosing and deleting data. If you process data on behalf of employees or customers, GDPR applies. GDPR is technology neutral - this means it protects the personal data of data subjects regardless of the technology used or how the personal data is stored. It applies to both electronic and paper-based files

Personal data is any information that identifies a data subject. For example, it includes their:

* Name
* Address
* Telephone number
* Email address, including corporate e-mail addresses that have individual names e.g: john.murphy@google.ie
* Date of birth
* Online identifiers such as an IP address and location data

There are six legal bases for processing personal data:

* Consent
* Legal obligation
* Contractual obligation
* Vital interests
* Public interests
* Legitimate interests

There are additional requirements for processing sensitive data. (see further reading section) Sensitive data is personal data that relates to a person’s profile including their:

* Race or ethnicity
* Political, religious or philosophical beliefs
* Sexual life or sexual orientation
* Health
* Genetic or biometric data
* Criminal record
* Trade union membership

The organisation should ask itself whether it processes personal or sensitive data on behalf of employees, volunteers, members, or any other stakeholders. If the answer is yes then GDPR applies, and data protection guidelines should be in place. The organisation should examine all areas of its work to understand where and when personal data is processed, in order to build the best guidelines.

Data protection checklist

**The following is a checklist for an organisation to undertake in developing data protection guidelines:**

* Assess the risk level – the organisation needs to assess what is the risk level of the data processing activities and what harm could be caused to individuals if the data was breached e.g. damage to reputation, identity theft or fraud, etc. Depending on the risk level and potential harm caused if personal data is compromised, the organisation will need to assign the appropriate organisational measures (people and processes) and technical measures (IT and security) to safeguard and protect personal data
* Assign responsibility - Assign someone within the organisation to implement and be responsible for the ongoing compliance of GDPR. They should have sufficient support and resources to do this. The organisation may need to appoint a Data Protection Officer.
* Record the data - Make an inventory of all the personal data that the organisation processes using the following headings:
  + Types of data?
  + How did we obtain it?
  + Why was it originally gathered?
  + How long will we retain it?
  + How secure is it, both in terms of encryption and accessibility?
  + Do we ever share it with third parties and on what basis might we do so?
* Categorise the data – is the data personal or sensitive?
* Assign a legal basis - organisations must assign at least one or more legal bases to the personal data they process (as per the six legal bases for personal data or ten for sensitive data).
* Set the retention period - GDPR states that data should only be held for as long as necessary but does not specify how long it should be held. Organisations should decide this themselves, with an objective justification as to how long they might hold it.
* Manage consent – under GDPR consent must be freely given, specific, informed and unambiguous. So, for example, when collecting peoples email addresses, e.g., in a survey or email, written consent notices must be separate from other notices, and be in an easily accessible form using clear and plain language. The data subject has the right to withdraw consent at any time.
* Update consent notices - Silence, pre-ticked boxes or implied consent are not allowed under GDPR.
* Update privacy notices – e.g., on the website and email make sure to include the name and contact details of the business, the purpose for using the data, the use(s) that the data will be put to, etc.
* Review contracts with third party suppliers - If the organisation outsources the processing of personal data to a data processor such as a cloud services company, credit card supplier or other service provider it must ensure that they comply with GDPR and have a specific Data Processor Agreement in place
* Manage data access requests - access requests by data subjects must be processed within one month.
* Keep data secure – organisations need to ensure that both their organisational and technical measures safeguard and protect personal data.
* Staff and volunteer training - staff and volunteers should be trained on:
  + What is data protection
  + Policies and procedures in relation to data protection
  + How to recognise and act upon a data access request
  + Keeping personal data secure
  + Following correct IT and organisational procedures and guidelines
  + Following the correct procedure in relation to a data breach
* Prepare for data breaches - Have a data breach response plan in place and test it
* Review and refresh – organisations should regularly check their data protection guidelines to ensure they are up to date, and moving in line with the organisation

Implementing data protection: how and when to use it

New staff and volunteers should be made aware of all policies during the induction process, including the data protection guidelines, and this should also be included in the employee handbook, and any introductory documentation given to volunteers. Data protection could be included in any IT training initiatives to make sure everyone within the organisation - from the Board, to the volunteers and administrative teams - knows and understands the guidelines. The guidelines should be regularly reviewed – the Code states that policies must be reviewed every 3 years – organisations may choose to review their data protection more regularly than that given that it is an area that is subject to legislation.

Further links and resources

[Data Protection Commission](https://www.dataprotection.ie/)

[Data Protection Commission - Self-Assessment Checklist](https://www.dataprotection.ie/en/organisations/resources-organisations/self-assessment-checklist)

[Data Protection Commission - DPOs](https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officers)

[Data Protection Commission- Legal Basis](https://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data)