



*The voice of Irish sport*

## **Federation of Irish Sport**

### **Personal Data Breach Procedure**

#### **Introduction**

As an organisation that processes personal data the Federation of Irish Sport must ensure appropriate measures are in place to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The General Data Protection Regulation (GDPR) specifies that all breaches which are likely to result in a risk to the rights and freedoms of natural persons should be reported to the Office of the Data Protection Commissioner (ODPC) *“without undue delay...not later than 72 hours after having become aware of it”*.

In the event of a data breach or an information security incident, it is therefore vital that appropriate actions are taken to promptly report the breach to the Federation of Irish Sport CEO (Mary O’Connor – [mary.oconnor@irishsport.ie](mailto:mary.oconnor@irishsport.ie)) who will manage the incident and minimise associated risks.

This document sets out the guidance and procedure for personal data breach incidents and must be read in conjunction with the Federation of Irish Sports Data Protection Policy.

#### **Purpose and scope**

The purpose of this procedure is to provide a consistent and effective framework within which the Federation of Irish Sport will ensure compliance with the legislative requirements of managing a personal data breach incident, or suspected or confirmed.

This procedure applies to the Federation of Irish Sports employees, agents, contractors or other parties who process data for or on behalf of the Federation of Irish Sport and it must be complied with in the event of a personal data breach.

The Federation of Irish Sport is required to keep a record of all security incidents involving personal data. It is vital that all staff report a personal data breach or suspected personal data breach, however minor as soon as possible after discovery, so that we can use the permitted 72 hours to establish what has happened, the size of the breach and whether it needs to be reported further.

This procedure has been designed to ensure that:

- Data breach events are detected, reported and monitored consistently.



*The voice of Irish sport*

- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of a breach.
- Relevant breaches are reported to the Office of the Data Protection Commissioner (ODPC) within the 72 hour window.
- Improvements are made to prevent recurrence.
- Lessons learnt are communicated to all Federation of Irish Sport employees, agents, contractors or other parties who process data for or on behalf of the Federation of Irish Sport.

### Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access to personal data.

A personal data breach can happen for a number of reasons, some of which are outlined below:

- Loss or theft of data or equipment on which data is stored, or through which it can be accessed.
- Loss or theft of paper files
- Hacking attack
- Inappropriate access controls allowing unauthorised/ unnecessary access to data
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood

### Reporting an incident

It is vital that as a Personal Data Breach is identified or suspected it is immediately reported to the Federation of Irish Sport CEO (Mary O'Connor – [mary.oconnor@irishsport.ie](mailto:mary.oconnor@irishsport.ie)). The longer an incident goes unreported, the harder it gets to resolve any vulnerabilities.

Impacted data subjects have a right to know that their data may have been compromised and that they could then take steps that could minimise an adverse impact on them such as informing their bank that their bank details have been compromised.



*The voice of Irish sport*

Any delay in reporting allows the incident to escalate or for further consequential incidents to occur. Without timely visibility of the incident through reporting the Federation of Irish Sport may not be able to fulfil its legal obligations. The EU General Data Protection Regulations (GDPR) places a duty on organisations to report certain types of personal data breach to the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of the breach.

Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust to prevent future breaches and protect personal data.

Responsibility for reporting a suspected breach lies with the person who discovered the potential breach. As much information as is immediately available should be collated and sent to the Federation of Irish Sport CEO (Mary O'Connor – mary.oconnor@irishsport.ie) as soon as possible via email and within 12 hours of the breach being identified at the very latest.

The Federation of Irish Sport CEO will analyse the information sent via email regarding the breach, update the personal data breach log and ascertain whether any immediate corrective/ containment/ escalation actions are required.

### Investigating an incident

Depending on the type and severity of the incident the Federation of Irish Sport CEO (Mary O'Connor) will assess whether a full investigation into the breach is required. Where required a full breach report will be compiled.

The investigation will:

- a) Establish the nature of the incident, the type and volume of data involved and the identity of the data subjects.
- b) Consider the extent of a breach and the sensitivity of the data involved.
- c) Perform a risk assessment.
- d) Identify actions the organisation needs to take to contain the breach and recover information.
- e) Assess the ongoing risk and actions required to prevent a recurrence of the incident.



*The voice of Irish sport*

### Reporting a breach to the ODPC and data subjects

The Federation of Irish Sport CEO will co-ordinate breach reporting to the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of the relevant breach. Evaluation of whether the breach is *"likely to result in high risk to the rights and freedoms"* of the data subject. If this is determined to be the case, the incident will also be reportable to the data subject(s) involved without undue delay.

### Associated documents and policies

This policy is to be read in conjunction with the Federation of Irish Sports other policies:

- Privacy Policy
- Data Protection Policy
- Data Retention Policy
- Data Subject Access Request Procedure Policy

### Enforcement

Failure to adhere to this procedure, whether it be by delay or failure to report the breach to the Federation of Irish Sport CEO (Mary O'Connor) may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

Policy has been approved



*The voice of Irish sport*

This policy will be reviewed and updated on an annual basis, or sooner if deemed necessary.

This policy has been approved and authorised by:

**Name:** Mary O'Connor

**Position:** CEO Federation of Irish Sport

**Date:** 25<sup>th</sup> May

**Signature:**