DATA PROTECTION POLICY

VERSION HISTORY

Version Number	Date
1.2	06/03/2019

POLICY STATEMENT

Everyone has rights with regard to how their personal information is handled.

INTRODUCTION

During the course of our activities the Olympic Federation of Ireland (OFI) will collect, store and process personal information and the OFI recognises the need to treat it in an appropriate and lawful manner.

OFI is committed to doing so in a manner that complies with data protection law and respects the privacy rights of individuals. OFI may be required to handle details of current, past and prospective employees, volunteers, management, members, contractors, suppliers and others that we communicate with. The information may be held on paper or online and is subject to certain legal safeguards specified in the General Data Protection legislation (GDPR).

This Data Protection Policy ("**DP Policy**") is designed to give practical guidance and raise awareness on OFI's approach to data protection law and on how to comply with data protection responsibilities.

This document will give a broad overview of:

- Data protection laws and principles
- Data Subject's rights
- Basis for processing data
- OFI Staff obligations
- Data Breaches
- Data Subject Access Requests
- Data Retention

This DP Policy is a guidance document only. It is not a summary of the law or an exhaustive list of your data protection responsibilities.

DATA PROTECTION LIAISON

We have appointed a data protection liaison (DPL) with overall responsibility for data protection within the OFI. Any questions or concerns about this policy should be referred in the first instance to the DPL at admin@olympicsport.ie. Where appropriate, please also refer to the website of the Office of the Data Protection Commissioner at www.dataprotection.ie for any further information.

DEFINITIONS

The following definitions are used in this Policy:

"Data" is information which is stored electronically, on a computer, or in structured paper-based filing systems.

"Data Breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, as defined per GDPR.

"Data Controller" is the person who or organisation which determines the purposes for which, and the manner in which, any personal data is processed. As a data controller, the OFI has a responsibility to establish practices and policies in line with GDPR legislation.

"Data Protection Commissioner (DPC)" The Office of the Data Protection Commissioner is the independent national authority responsible for upholding the EU fundamental right to data privacy

through the enforcement and monitoring of compliance with data protection legislation in Ireland.

Data Subject An identified or identifiable natural person whose personal data is being collected, held or processed.

"Data Subject Access Requests (DSAR)" A DSAR is a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under GDPR.

"Data users" include employees or volunteers whose work involves using personal data. Data users have a duty to protect the information they handle by following this data protection policy at all times.

"Data processors" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Where the OFI works with outside bodies or organisations and only process personal data on their behalf and under their instruction we may be the data processor of that organisation's personal data.

"EEA" means the European Union member states, Iceland and Liechtenstein, Norway.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); who can be identified, directly or indirectly by reference to the data.

"Processing" is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any action using the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

"Sensitive personal data" data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

GENERAL DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the six broad principles of data protection. These provide that personal data must be:

1. obtained and processed fairly **("fair processing");**
2. kept for a specified and lawful purpose or purposes and not processed in any way incompatible with those purposes **("purpose limitation");**
3. kept safely and securely **("integrity and security");**
4. kept accurate, complete and up to date **("accurate data");**
5. adequate, relevant and not excessive for the purpose it was collected **("data minimisation");**
6. not kept longer than necessary for the purpose or purposes **("storage limitation");**

1. Fair Processing

The purpose of implementing the GDPR Legislation is not to prevent the processing of personal data, but to ensure that it is done fairly and without negatively affecting the rights of a data subject.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for our legitimate interest. Where an individual fills out a competition entry form, then it is implied that they consent to us having this information to process their entry. However, if the OFI wanted to use that personal data for another purpose, for example, to pass it to a third party, the OFI would need to ask the individual for consent to this.

Where an outside organisation seeks to transfer personal data or sensitive personal data from its members, customers or suppliers to us, the OFI must first ask that outside organisation to ensure that it is entitled to transfer that data to us and, where relevant, that it has obtained the consent from the relevant data subjects to the transfer to us. If an outside organisation proposes to transfer third party personal data to us and you are unsure whether you should accept such information, please contact the DPL for assistance.

2. Purpose Limitation

Personal data may only be kept and processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Acts. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose and written consent must be sought before any processing occurs.

3. Integrity and Security

The OFI must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. GDPR legislation requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection through to the effective and safe destruction of that personal data. Maintaining data security also means ensuring that the personal data is kept confidential. Only people who are authorised to access or use personal data should have access to it. This can be achieved by storing physical data in a filing cabinet or room that can be locked and the key is kept securely by one authorised person who can monitor access. On a computer security can be achieved by using document passwords and limiting access to shared folders.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. Hard disc storage devices and other electronic storage devices should be physically destroyed when they are no longer required.
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- Portable Devices. Portable devices include smartphones, tablets, laptops or other mobile devices that can be used to store or access data. Data users must ensure that portable devices used in the course of working with us (whether belonging to your NGB, any third party, or the user) that may contain personal data are kept safe and secure. A password should be maintained on all devices. Where any portable device that may contain personal data is stolen or lost, this should be reported to the DPL immediately.

4. Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

5. Data Minimisation

Personal data should only be collected for the specific purpose notified to the data subject. Any data

which is not necessary for that purpose should not be collected in the first place.

6. Storage Limitation

In the absence of any legal requirement, personal data should not be kept longer than is necessary for the reason it was collected. This means that data should be destroyed or erased from our systems when it is no longer required. For example, when a person is no longer competing, the OFI should not keep prior information collected on him or her indefinitely and, after a certain period, the OFI will have to delete it. The following are our maximum data retention periods which should be calculated from the end of the calendar month following the last entry or activity on the file or document:

TYPE OF INFORMATION	MAXIMUM RETENTION PERIOD	HOW TO DESTROY/ARCHIVE
Participant data including contact details, emails and correspondences	5 years from departure from active competition	• Archive in a secure location with limited access after 12 months since previous competition • Shred physical files and delete from IT systems, address books, mobile phones after 5 years
Medical Records	2 years	• Shred physical files and delete from IT systems after 2 years
Statistics, results, member images and video footage	This information will be retained indefinitely in a secure archived form in the public interest, and in the interest of archiving, historical research, or statistical purposes / in the legitimate interest of promoting the sport.	• Archive in secure location with limited access, as advised by DPL.
Documents relevant to current or potential litigation, investigations, inquiries	DO NOT DESTROY	• CEO retains • Copies of Identification documents, 'Garda Vetting applications' and positive disclosures • Under Irish Law there is a positive obligation to preserve documents where litigation is anticipated or ongoing. These documents must be preserved and not destroyed

SENSITIVE PERSONAL DATA

Sensitive Personal Data is afforded “special category” status under GDPR, meaning OFI can only process it on the following grounds:

- the individual has given their explicit consent to the processing;
- the processing is necessary for the performance of our obligations under employment law;
- the processing is necessary to protect the vital interests of the data subject (i.e. a life or death or other extreme situation);
- the processing relates to information manifestly made public by the data subject;
- the processing is necessary for the purpose of establishing, exercising or defending legal claims; or
- the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

Access to Sensitive Personal Data must be restricted to those who specifically need to access it. Physical records should be stored in locked filing cabinets. Electronic records should be encrypted with a password that is only known to those who need to access it. Those who do not need to access sensitive personal data are prohibited from accessing it.

DATA SUBJECTS' RIGHTS

Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are

- The rights to access their personal data, usually referred to as a subject access request;
- The right to have their personal data rectified;
- The right to have their personal data erased, usually referred to as the right to be forgotten;
- The right to restrict processing of their personal data;
- The right to object to receiving direct marketing materials;
- The right to portability of their personal data;
- The right to object to processing of their personal data; and
- The right to not be subject to a decision made solely by automated data processing.

Not all of these rights are absolute rights. Some are qualified and some only apply in specific circumstances. Where an individual requests updates or otherwise receives marketing emails from us, then each communication to that individual should contain instructions on how to opt-out of receiving further communications.

Where an individual requests access to their personal data, the procedures per the DSAR procedures listed below should be followed: Where an individual does opt-out, the OFI should ensure that no further marketing communications are sent to that individual

Providing Information Over the Telephone

OFI Personnel will not provide Personal Data over the phone unless we are sure we have the right to do so. In particular, we will:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
- Refer to the DPL for assistance in difficult situations. No-one should be pressured into disclosing personal information

OFI STAFF MAIN OBLIGATIONS

What this all means for OFI Staff can be summarised as follows:

- Treat all personal data with respect;
- Take care with all Personal Data and items containing Personal Data so that it stays secure and is only available to or accessed by authorised individuals; and
- Immediately notify the DPL if:
    - There is any suspicion of the loss or breach of any Personal Data (see Data Breach Policy below for more details)
    - There is any suspicion that any individual is breaching or has breached data protection laws, or this policy
    - An individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to Personal Data relating to them;

- Any breaches of this Policy will be viewed very seriously and may be dealt with under disciplinary procedures.

POLICY AMENDMENTS and NOTIFICATIONS

This document may be amended from time to time by the Board or by officers of the OFI authorised by the Board to do so. The definitive text of this document in force from time to time is the version contained on OFI server under Governance Policies. Any printed text or electronic copy held elsewhere is only a snapshot of the text at the time it is printed, copied or downloaded.

CONTACT

Questions, comments and requests regarding this policy are welcomed and should be made to the DPL at admin@olympicsport.ie

SCHEDULES

1. FOREIGN TRANSFERS OF PERSONAL DATA

a) As a general rule, personal data must not be transferred outside the European Economic Area (**EEA**) unless you are satisfied the destination country has an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections.

b) As set out in our Privacy Policy, reasonable steps and assurances should be sought from countries to ensure that our normal security measures and protections apply. If you are involved in any new processing of personal data, particularly where sensitive personal data is involved, which may involve transfer of personal data outside of the EEA, then please seek the prior approval of the DPL.

2. DATA BREACH POLICY (to be read in conjunction with Computer, Internet and email policy)

Even with the best designed systems, mistakes can happen. When a data breach occurs, it is essential to respond in accordance with procedure. (Note: as data controller we are obliged to inform the DPC within 72 hours of becoming aware of the breach and any data subjects if there is a high risk that they will be adversely affected by the breach. Consideration should be given to this risk.)

Data Breach Incident Response Procedure

Step 1: Contain the breach

(i) Notify the DPL
(ii) Immediately contain breach (e.g. Shut down/ disable relevant emails / server infrastructure and or disable connectivity)
(iii) Consider whether the DPL needs other expertise
(iv) Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing OFI to take appropriate corrective action
(v) Consider a communications strategy

Step 2: Assess the risks for individuals associated with the breach

Conduct initial investigation, collect and document information about the breach promptly, including:

(i) the date, time, duration, and location of the breach
(ii) the type of personal information involved in the breach
(iii) how the breach was discovered and by whom
(iv) the cause and extent of the breach
(v) a list of the affected individuals, or possible affected individuals
(vi) the risk of serious harm to the affected individuals
(vii) the risk of other harms
(viii) determine whether the context of the information is important
(ix) establish the cause and extent of the breach
(x) assess priorities and risks based on what is known
(xi) Keep appropriate records of the suspected breach and actions of the DPL, including the steps taken to rectify the situation and the decisions made

Step 3: Consider breach notification

(i) Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage
(ii) Determine whether and how to notify affected individuals. Is the breach likely to result in serious harm to any of the individuals to whom the information relates and if OFI has been able to prevent the likely risk of serious harm through remedial action. In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals
(iii) If a breach is confirmed, a formal notification to the DPC is required within 72 hours
(iv) If there is a significant risk to the subject's data privacy - a formal notification to data subjects is required
(v) Consider whether others should be notified, including suppliers, customer, regulatory authorities

Step 4: Review the incident and take action to prevent future breaches

(i) Fully investigate the cause of the breach
(ii) Implement a strategy to identify and address any weaknesses in data handling that contributed to the breach
(iii) Conduct a post-breach review
(iv) Update security and response plan if necessary
(v) Make appropriate changes to policies and procedures if necessary
(vi) Revise staff training practices if necessary
(vii) Consider education sessions with Staff, if required
(viii) Consider the option of an audit to ensure necessary outcomes are affected
(ix) Complete the Data Breach Log

3. DATA SUBJECT ACCESS REQUESTS (DSARS)

Data subjects have the right to make a **DSAR.**

The **DSAR** may be for all personal data of that data subject held by OFI or a subset of the data. OFI must respond to the request within 1 month, unless OFI can show that the request is manifestly unfounded or excessive, or where the request is sufficiently complex, or one of a number of requests, or where the identity of the requestor is unclear (in which case the response time may be extended). OFI cannot charge a fee for processing this request, unless OFI can show that the request is manifestly unfounded or excessive.

Where the OFI receives a **DSAR:**

(i) It shall be immediately referred to the DPL.
(ii) OFI will conduct due diligence to confirm the identity of the data subject. The OFI will not comply with DSARs made by anyone other than the data subject him/herself. This will typically involve seeking a copy of passport or drivers licence to prove identity.
(iii) OFI will assess all data held on behalf of the individual, including data held on the OFI 's central data server, laptops and personal computers in the OFI, stored emails and other electronic messaging systems and paper files
(iv) All data relating to any individuals other than the maker of the request will be redacted.

The OFI will consider whether its legal and professional obligations require any data held by the OFI to be kept confidential or retained in some form/fashion due to competing retention requirements. Records of all DSARs and response times shall be kept by the OFI in a DSAR register.