INCLUSIVE SKATING

Data Protection Officer Appointment

*This note is designed to provide guidance to Inclusive Skating Charity Trustees in determining whether or not it is required under the General Data Protection Regulation (**GDPR**) to appoint a Data Protection Officer (**DPO**). For more detailed guidance, please visit https://ico.org.uk.*

Do we need to appoint a Data Protection Officer?

Under the GDPR, you **must** appoint a DPO if:

- you are a public authority (except for courts acting in their judicial capacity) *(see clause 1.1 below);*
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking) (*see clauses 1.2 and 1.3 below)*; or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences (*see clause 1.4 below).*

(Article 37(1), GDPR.)

Both data controllers and data processors *(defined below)* are subject to Article 37 of the GDPR and may be required to appoint a DPO.

*A **data controller** is defined as 'a natural or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the*

processing of personal data' whereas a data processor is defined as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller'. So a data controller is the person that controls how the data is used and processed. For example, an employer will always be a data controller of personal data relating to its employees.

*A **data processor** is a person who processes the personal data in accordance with the instructions of the data controller. They are usually a supplier to the data controller, but not all suppliers are data processors. For example an outsourced payroll provider will be a data processor, as they will process the payroll information they are provided with by the employer strictly in accordance with the instructions of the data controller. However a health insurance provider providing health insurance to the employer's employees would be a data controller because, although they are supplying a product to the employees of the employer, they will decide how they use and process the personal data they are provided with in order to provide the insurance product.*

Whether you need to appoint a DPO depends on whether your organisation meets any of the three conditions above. There is no definitive answer that can be applied across the whole sports sector and whilst it is likely that most clubs and smaller-scale national organisation will not need to appoint a DPO, you still need to consider whether your organisation meets any of the above conditions.

You can appoint a DPO if you wish, even if you aren't required to, but if you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory under the GDPR.

1.1 What is the definition of a public authority?

The Data Protection Bill defines what a 'public authority' is under GDPR. This is the same as those defined under the Freedom of Information Act 2000 (FOIA) or the Freedom of Information Act (Scotland) 2002.

This means that if you are already defined as a public authority or public body under FOIA or the Scottish FOIA, it's likely you will be a public authority under the GDPR. However, the Data Protection Bill is subject to amendment and so you should confirm your status when the Bill becomes an Act of Parliament.

1.2 What are 'core activities'?

The other two conditions that require you to appoint a DPO only apply when:

- your core activities consist of processing activities, which, by virtue of their nature, scope and/or their purposes, require the regular and systematic monitoring of individuals on a large scale; or
- your core activities consist of processing on a large scale of special category data, or data relating to criminal convictions and offences.

Your core activities are the primary business activities of your organisation. So, if you need to process personal data as part of your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (e.g. payroll or in relation to employing your staff), but which is not part of carrying out your primary objectives.

Consider what are the key objectives for your organisation? If for example, you are an organisation who as part of their key objectives, works with and supports disabled individuals

to stay active in sport, you may be processing special categories of data on a large scale and be required to appoint a DPO *(see below for definition of special category of data).*

1.3 What does 'regular and systematic monitoring of data subjects on a large scale' mean?

1.3.1 Regular and Systematic

Although the GDPR does not define 'regular and systematic monitoring' or 'large scale', the Article 29 Working Party (which was set up to provide the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States) interprets "**regular**" as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period.
- Recurring or repeated at fixed times.
- Constantly or periodically taking place,

and interprets "**systematic**" as:

- Occurring according to a system.
- Pre-arranged, organised or methodical.
- Taking place as part of a general plan for data collection.
- Carried out as part of a strategy.

It also provides some examples of "**regular and systematic monitoring of data subjects**", which include:

- Operating a telecommunications network.
- Providing telecommunications services.
- Data-driven marketing services.
- Profiling and scoring for the purposes of risk assessment (for example, for the purposes of credit scoring, the establishment of insurance premiums, fraud prevention or the detection of money laundering).
- Location tracking.
- Loyalty programmes.
- The use of connected devices (for example, smart meters, smart cars, home automation and so on).

1.3.2 Large-scale processing

Whilst the GDPR does not indicate what qualifies as "large scale", the Article 29 Working Party Guidance (**WP29 Guidance**) recommends considering the following factors when determining whether processing should be considered to be carried out on a large-scale:

- The number of data subjects concerned, either as a specific number or as a proportion of the relevant population.
- The volume of data and/or the range of different data items being processed.
- The duration, or permanence, of the data processing activity.

- The geographical extent of the processing activity.

The WP29 Guidance also provides a range of examples of large-scale data processing, which include:

- Processing of travel data of individuals using a city's public transport system (for example, tracking through travel cards).
- Processing of customer data in the regular course of business by an insurance company or a bank.
- Processing of personal data for behavioural advertising by a search engine.

1.4 What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?

Processing special category data *(i.e. information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)* or criminal conviction or offences data carries more risk than other personal data.

Examples of processing special categories of data or criminal conviction or offences may include collection of any medical or disability information from participants to assess their suitability for an event or storing criminal record history on coaches or volunteers to comply with safeguarding obligations. So when you process this type of data on a large scale as part of your core activities you are required to appoint a DPO, who can provide more oversight.

Again, the factors relevant to large-scale processing can include:

- the numbers of data subjects;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the activity.

1.5 What qualities must a DPO have?

Where you are required or voluntarily decide to appoint a DPO, the DPO should be appointed on the basis of their professional qualities and expert knowledge of data protection law and practices. WP29 Guidance recommends that all appointed DPOs should meet the following qualities and expertise:

- Expertise in national and European data protection laws and practices, including an in-depth understanding of the GDPR.
- Understanding of the processing operations carried out.
- Understanding of information technologies and data security.
- Knowledge of the business sector and the organisation.
- Ability to promote a data protection culture within the organisation.
- Personal qualities including integrity and high professional ethics.

1.6 **Who can we appoint as a DPO?**

Rather than you having to create a new position, an existing employee can be appointed as a DPO as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. An external DPO may also be appointed by means of a service contract.

In any event, the WP29 Guidance stresses the importance of ensuring that the DPO is protected by the provisions of the GDPR, in particular ensuring no unfair termination of a service contract for activities as DPO or dismissal of any individual member of the organisation for carrying out tasks as a DPO.

1.7 **What do we have to do to support the DPO?**

If you do appoint a DPO, the GDPR requires that the DPO is involved in all issues relating to the protection of personal data, from ensuring the data protection principles are respected to preserving data subject rights, recording data processing activities and ensuring the security of processing. To do this, the GDPR requires that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. The following factors should be considered:

- Senior management support.
- Time for DPOs to fulfil their duties. This is particularly relevant for DPOs appointed on a part-time basis or external appointments.
- Adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate.
- Official communication of the designation of the DPO to make known existence and function within the organisation.
- Access to other services, such as HR, IT and security, who should provide support to the DPO.
- Continuous training so that DPOs can stay up to date with regard to data protection developments.
- Where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member.

1.8 **Alternatives to the appointment of a DPO**

- Where an organisation is required by the GDPR to appoint a DPO, failure to do so exposes it to a fine of up to EUR10 million or 2% of the previous year's total worldwide turnover, whichever is higher. Therefore any private organisation that decides against appointing a DPO should consider the requirements and the rationale for declining the appointment and ensure that these are documented and filed with other data protection records. Keeping a record of any justification for not appointing a DPO will be important in the event that this is queried by a supervisory authority.
- Regardless of whether the GDPR obliges you to appoint a DPO or not, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR and your organisation should still designate data protection responsibilities to an internal appointment or external service provider.
- To avoid being made subject to the DPO provisions of the GDPR, however, organisations must ensure that there is no confusion over whether the role can be

regarded as a DPO e.g. do not assign the title "data protection officer" to an appointment if the individual is not in fact a DPO. Instead choose a title that is not likely to be confused with that of DPO.

- Also the organisation can consider implementing a GDPR working group to reduce the risk of issues while the individual responsible for data protection compliance in your organisation is on annual leave or decides to leave the organisation.