Background Paper

EUROPEAN OLYMPIC COMMITTEES | EU Office

Sport and the General Data Protection Regulation (GDPR)

May 2018

Background Paper

EUROPEAN OLYMPIC COMMITTEES | EU Office

On **25 May 2018**, the new EU Data Protection Law Enforcement Directive and General Data Protection Regulation (GDPR) will come into force. The application of the GDPR will fundamentally change the way sport organisations are allowed to collect and process data of their members (e.g. athletes, staff) and third parties.

As the main objective of this new package is to better protect the data of EU residents, these EU rules will also impact sport organisations based outside the EU in so far as they collect and process data of people based in the EU territory.

The present document does not aim to provide sport organisations with specific legal recommendations on the way to adapt their rules to the new legal situation, but to underline potential areas in which actions might be necessary to be in line with EU GDPR.

Table of contents

I. Overview of the General Data Protection Regulation (GDPR)

A. Background

The protection of personal data is a fundamental right for EU citizens. It is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union[1], which defines that everyone has the right to the protection of personal data and to access data which has been collected and the right to have it rectified.

The regulation deals with the processing of personal data. The new data protection package, which will come into force on 25 May 2018, was proposed by the European Commission in 2012 and adopted in April 2016 after intense discussions both in and between the European Parliament (EP) and the Council. Regulation (EU) 2016/679, the European Union's ('EU') new General Data Protection Regulation ('GDPR')[2], regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.

B. Objectives

The GDPR is set up to fulfil the following aims:

- Protecting EU citizens in the global economy, adapting it to the internet and other new technologies and having rules applicable to any company, no matter where it is based, that processes the personal data of EU residents.
- Giving individuals full control over their personal data, by putting free consent as a central piece and giving citizens better control of what they share and for what purposes.
- Stronger protection against data breaches and improved levels of compliance, by introducing significant penalties, including potential fines of up to 4% of annual global turnover, or EUR 20 million, whichever is greater.
- Allowing new business opportunities, through a harmonised legal framework in the single market as well as clearer rules for international data transfers.

The Regulation is directly applicable in all the Member States even if several concrete elements still need to be defined at the national level by adapting national legislations.

All sport organisations, including those based outside the EU, that deal with personal data of EU residents will have to comply with the new GDPR.

[1] **Charter of Fundamental Rights of the European Union**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[2] **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance),** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

II. Check-list for sport organisations

In the following points, the EOC EU Office aims to give an overview of some aspects sport organisations should consider in order to verify their application of data protection rules and to prepare themselves for the new legal system.

A. Is my organisation concerned by the new GDPR?

All sport organisations, such as National Olympic Committees, international, European and national federations, clubs or anti-doping agencies, which collect, store and process the personal data of their members and other persons including spectators, sponsors, insurances, suppliers working in EU area will be concerned by the new GDPR.

This applies irrespective of the country of establishment of the organisation as all organisations collecting and treating data of EU residents have to comply with the rules, even if they are based outside of the EU.

> Sport organisations based outside the EU (e.g. Non-EU NOCs, European and International federations):
>
> All sport organisations, including orgaisations based outside the EU, dealing with personal data of EU residents will have to comply with the new GDPR. In other words, the processing of personal data falls under the scope of the GDPR insofar as it targets data subjects in the EU, such as spectators, officials, staff or athletes that are training or competing within the European Union.
>
> In addition, Article 27 GDPR sets out the obligation for non-EU based entities which fall under the territorial scope of the GDPR to designate in writing a representative in the Union. The representative shall be mandated to deal with supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with the GDPR.

B. Which of my activities are considered as data processing?

All activities leading to the collection (e.g. mailing list of fans, spectators), the use (e.g athletes diets or performance) and/or the transfer and communication (e.g. sensitive data to protect the integrity of competition) could potentially be considered as data processing.

In the context of a sport organisation such data could be:

- Personal data of sport club members;
- Personal data of third parties (such as spectators at sport events, sponsors,…);
- Personal data of employees;
- Personal data of subscribers of an email newsletter;

In the case of sensitive data, such as genetic data, health data or opinions and beliefs, special, stricter requirements apply to the processing of them (see below under question D).

C. Are responsibilities regarding treatment of data well established in my organisation? Do I have to nominate a person in charge of internal data protection rules?

The first step is to map out your current data processing activities and re-evaluate your internal processes. In particular, you must identify which data you hold and for what purpose and on what legal basis you hold it (see question D). All relevant employees of your club or federation should be informed of the necessity to adapt to the new data protection rules.

An overview of your data processing activities (directory of data processing operations) covering information on which data is collected of whom for which purposes as well as who is responsible should be established. **The creation of a registry including a description of all the data processed, their purpose, and the persons concerned is recommended for all sport organisations.**

In addition, the nomination of a Data Protection Officer (DPO) responsible for monitoring the compliance of your sport organisation with the GDPR could also be required – conditions on when this is necessary may vary according to your national regulations. A DPO can be a member of staff holding other posts or a hired contractor. Your organisation needs to ensure that no other tasks could create a conflict of interest for the DPO.

D. Is the legitimacy of all data processing in the organisation assured?

Organisations have to check and ensure that the legitimacy of all data processing is based on one of the following legal bases (ART.6).

- the person concerned has given his or her **free consent** for the personal data to be processed. It should be a specific, informed, active and unambiguous consent with a clear right to withdraw it.
- if it is "*necessary for the performance of a task carried out **in the public interest** or in the exercise of official authority vested in the controller*". However this ground will apply only where the task carried out is defined as a matter of public interest in Union law or Member State law to which the controller is subject. Some Member States have defined the fight against doping as a matter of public interest through national laws – the national status quo regarding this matter was the topic of a Commission Study last year[3].

[3] European Commission: „Study on anti-doping and data protection", 19 October 2017: https://publications.europa.eu/en/publication-detail/-/publication/50083cbb-b544-11e7-837e-01aa75ed71a1/language-en/format-PDF/source-44694285.

- if "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party".* Fight against corruption could be an example of legitimate interest depending national legislations.
- if the processing is necessary for the execution of a contract to which the person concerned is a party (e.g. membership card or licence, spectator buying a ticket);

Processing general data on sport competitions including participants, composition of the team or a delegation, sport results or ranking should also be based on a legal basis. **In that perspective, we would recommend your organisation to establish a template for a consent form to be signed by athletes or officials participating in your competition which covers the different use of the data you might make in the future.**

As long as the data are lawfully collected and treated, the publication and communication of these general data pose, in principle, no problem.

Fundamental rules to respect when processing data:

- *Lawfulness, fairness and transparency*: towards the data subject;
- *Purpose limitation*: for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- *Data minimisation*: adequate, relevant and limited to what is necessary in relation to the purposes;
- *Accuracy*: accurate and, where necessary, kept up to date;
- *Storage limitation*: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes;
- *Integrity and confidentiality*: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- *Accountability*: The controller is responsible for and has to be able to demonstrate compliance with these principles
- *Safety and confidentiality* of the data collected must be ensured. Any breache could lead to sanctions (see Question G)

E. Which type of requests can my organisation receive from individuals?

When receiving a request from an athlet, a fan or an official you should respond to this request within 1 month and free of charge for the individual.

These rights include:

- Request to access:

Right to access: request access to personal data, free of charge. If you receive such a request, then you have to:

  - tell the individual if you are processing their personal data;
  - inform them about the processing (such as the purposes of the processing, categories of personal data concerned, recipients of their data, etc.);
  - provide a copy of the personal data being processed.

- Request for data portability: obtain all the data in a commonly used and machine readable format.
- Request to erasure (right to be forgotten)

In this case, your organisation is obliged to delete all data saved for this individual. Exceptions do however exist in caseses where:

  - the processing is necessary to respect one's freedom of expression and information;
  - you must keep the personal data to comply with a legal obligation;
  - there are other reasons of public interest to keep the personal data, such as public health or scientific and historical research purposes;
  - you need to keep the personal data to establish a legal claim.

- request to correct for incorrect, inaccurate or incomplete personal data.

The question of sensitive data

In the case of **"sensitive data"**, which includes data revealing 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, only a limited number of legal grounds are available. This could be important within the context **of anti-doping, discussion on the gender of athletes, hormone rates, combating rules defining gender in sport or collection of performance and health data during training and matches.**

Potential legal basis are i.a.:

- Explicit consent;
- Substantial public interest;
- Public interest in the area of public health.

F. What should be taken into account in the contracts with third parties that handle data for you?

The GDPR imposes a high duty of care upon controllers in selecting their data processing service providers. Contracts with service providers such as event organisers, public authorities or private partners shall include a range of information (e.g. the data processed and the duration for processing) and obligations (e.g. assistance where a security breach occurs, appropriate technical and organisational measures taken and audit assistance obligations). It should be noted that contracts will potentially also have to be adapted for services that are not focused on data processing, but where the service provider would gain access to personal data – for example an IT company tasked to do maintenance work on computers or servers which would potentially give access to personal data. Sport organisations should therefore consider where they are working together with third parties that treat their data or could potentially have access and subsequently adapt these contracts to the new data protection rules.

G. What do I risk if I am not adapting my data protection rules? Do I have to notify a data breaches?

Fines might prove to be heavy as they can amount to 4% of turnover, within a limit of EUR 20 million. (Articles 82-84 GDPR)

In addition, all sport organisations are now subject to a general personal data breach notification regime. All breaches have to be reported to the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it. There are prescribed requirements to satisfy in the communication to the supervisory authority (e.g. describing the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned, etc.).

III. Overview

Review the privacy policy and fair processing notices of the club/ organisation to ensure that the transparency requirements are appropriately satisfied.

Determine who will be internally responsible for processing.

Carry out a Data Protection Impact Asssement to figure out what, how and why data is held by the club or organisation and to determine what the lawful purpose of collecting and holding that data. Establish a register of processing activities.

Establish a template for a consent form.

Consider if and under which legal basis any sensitive data is processed within your organisation.satisfied.

Review data security measures to ensure the safety and confidentiality of data. Establish appropriate systems in place in the event of a data protection breach.

Appoint, if necessary, a data protection officer.