GAISF
One Voice for all Sport

The importance of personal data protection

- Personal data are accessed and processed exponentially
- Abuse of personal data exploded
- Risk of data theft, piracy
- New « Cambridge Analytica » scandal almost every week

Need to establish higher standards of data protection and usage transparency

- For obvious moral reasons
- To keep/rebuild trust from individual vis-à-vis data processors

What is at stake

GDPR APPLIES TO THE *PROCESSING* OF *PERSONAL DATA* OF *DATA SUBJECTS*

Processing means: "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration*"
Personal Data means: any information relating to an identified or identifiable individual
Data subjects means: any individual concerned by the personal data being processed

GDPR **does not** aim at protecting business and/or manufacturing secrecy or any data related to an organization

Sport Associations process many personal data

- Athletes : licences, biographies, pictures, videos, biometrical data in the context of anti doping
- Followers/fans : newsletter, event attendance
- Media
- Employees, consultants, committees members
- Volunteers
- Coaches, medical staff and other non permanent staff

Extraterritoriality

"GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union*
- *the monitoring of their behavior as far as their behavior takes place within the Union*."

Six legal bases to process Personal Data

Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing 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;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Consent

Where relying on consent as the basis for lawful processing, ensure that:

- consent is active, and does not rely on silence, inactivity or pre-ticked boxes;
- consent to processing is distinguishable, clear, and is not *"bundled"* with other written agreements or declarations;
- supply of services is not made contingent on consent to processing which is not necessary for the service being supplied;
- data subjects are informed that they have the right to withdraw consent at any time but that this will not affect the lawfulness of processing based on consent before its withdrawal;
- there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;
- separate consents are obtained for distinct processing operations; and
- consent is not relied on where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).

The GDPR sets forth **six specific rights** for Data Subjects

1. **The right of acces/to be informed**

Who process your data, for what purpose, on which legal basis, which data, retention duration, …

You will have a month to comply, to a request to access. You can refuse or charge for requests that are manifestly unfounded or excessive.
If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.
If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.
In most cases you will not be able to charge for complying with a request.

2. **The right to object** : There are rights for individuals to object to specific types of processing:

- Direct marketing : The right to object to direct marketing is absolute (i.e no need to demonstrate grounds for objecting, no exemptions which allow processing to continue)
- Processing for research of statistical purpose. In the case of data collection for Scientific/historical/statistic purposes, there is an exception to the right to object where the processing is necessary for the performance of a task carried out for reasons of public interest.
- There are obligations to notify individuals of these rights at an early stage, clearly and separately from other information
- Online services must offer an automated method of objecting.

3. the right to data **portability** : The right to data portability is new.
    - It only applies:
        - to personal data an individual has provided to a controller;
        - where the processing is based on the individual's consent or for the performance of a contract;
        - and when processing is carried out by automated means.
    - You need to check if your data and associated meta data can easily be exported in structured, machine-readable formats so that it may be transferred by the data subject to another data controller without hindrance.
    - Look for industry initiatives to develop interoperable formats.

4. the right to **rectification**
5. the right to **erasure** (right to be forgotten)
6. the right to **restrict** processing

To fulfil these rights, data controllers and processors to adhere to the following general principles:

- lawfulness
- fairness
- transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality

Data breach

The GDPR introduces a duty on all organisations to report certain types of data breach to their controlling authority, and in some cases, to individuals. You only have to notify controlling authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

You may wish to assess the types of personal data you hold and document where you would be required to notify your controlling authority or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Privacy Impact Assessment

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the controlling authority to seek its opinion as to whether the processing operation complies with the GDPR.

Data Protection Officer

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.