What is the new EU GDPR? APPENDIX 17
How will it affect the ARISF International Federations, its National Federations and their Clubs and members?

New Data Protection Regulation

In the European Union (EU) a new General Data Protection Regulation EU 2016/679 (GDPR) has been approved and all handling of personal information has to be in-line with this regulation by the 25th of May 2018. Obviously, this will effect Sport quite a lot as well and it is essential that Clubs, National Associations and International Federations are prepared to take action in regards to this.

The National legislative bodies are in preparation of National Laws in this respect, but in a number of countries they have not yet been approved. This document tries to outline the content of the GDPR and how it in practise affects us in everyday life. The Global Association of International Sport Federations, is working on some General Guidelines and a workshop, but it is vital to provide information to our membership already now, as all might not be able to participate in common activities.

Who and what does the GDPR affect

The GDPR affects all, who inside the EU are dealing with personal information, regardless if it is single data or databases. It is important to notice that the GDPR also affects any organisation – even outside the EU – which manages or owns data from persons located in the EU. The GDPR is in force in both the public and private sector regardless of how much personal information is used, the nature of this information or the technology used. In all Sport organisations personal data is used and some kind of databases are made, which are used by a number of persons in that organisation.

Personal Data is all and every kind of data that directly or indirectly can be connected or attributed to a living natural person. It refers to all types of data, regardless of how it is stored. A person is considered a natural person, who can be identified directly or indirectly through the following personal data: name, national identification number, passport number, e-mail address, e-mail containing personal data, fingerprints, photos with identifiable persons, IP-addresses, vehicle registration number, GPS-data etc.

The GDPR defines so called high risk data as Sensitive Personal Data which includes Racial or ethnic origin, political opinion, religion or beliefs, trade union membership, health status, sexual orientation, DNA information, Biometric information

A Database is any kind of organised file containing personal data, where you can find information based on a search. All databases are a part of the GDPR, regardless of how they are built and what data they contain. For example, an excel-file made up of the referees or lecturers is considered a personal data database, as it contains personal information's. Also member, client or mailing lists are personal data databases, if they contain personal data. All data collected for the same reason are automatically part of the same database, regardless if they are stored electronically or partly on paper and they can be stored in different places.

What should Sport Organisations Do?

All Sport Organisations must before the 25th of May 2018 ensure, that all processing of Personal Data is in accordance with the GDPR inside the EU.

1) Conduct an Information Audit of the processing of Personal Data
   Make a survey and define how and what type of personal data you are collecting today and into which kind of databases and systems are used to store them. Who are collecting the data and what are they being used for. It is important to understand who are processing and using the data and for how long they are kept. Describe how data is deleted from the database.
   Please be aware of some of the outside organisations dealing with your data, like companies paying salaries or taking care of marketing communication.
   The organisation always have responsibility for the data, regardless of who is dealing with them.

2) Fulfil the requirements of the GDPR and prove it
   In accordance with the GDPR personal data shall be handled in a lawful, appropriate and for the person concerned transparent and meaningful purpose. The personal data shall be proper and essential and needs to be updated regularly. You may only use the personal data as long as your organisation has a lawful reason for using them and they have to be handle in a safe way, hindering any unauthorised or illegal use of them.

   Personal data may only be processed if it meets one of these legal grounds:

   - Legal obligation – when there is a legal obligation to process personal data

   - Performance of Contract – when the organisation has a contract with the data subject and prior to entering into a contract. This includes player and employee contracts and warranties

   - Vital interest – this is personal data necessary for organisations to fulfil responsibilities of interests for the data subject. This could be a player making a transfer or a member joining a club or association. Personal data for marketing is included here.

   - Consent means that a natural person has consented that the organisation can process it's data.
     The consent must be specific to the purpose, including transfer to a third party. Consent cannot be used in the relationship employer – employee

   You are responsible for the protection of the personal data from the gathering to the deletion of them. The protection requires that the processing is being followed and monitored. Protective measurements are for example the education of employees, guidelines for data handling, security measures for databases and encryption of data. The level of the security measures is dependent on the kind of personal data, the sensitivity of it and the risks that the processing can create.

3) Secure the Individuals' rights
   The GDPR gives the persons included in our databases much more rights than before. It defines how long you may store data, how to delete it and how and in which way you can share the information. Therefore, it is vital that we all are aware of what these rights of the Individuals' are:

- Right to be informed when data is collected
- Right to get access to their data
- Right to correct any mistake in their data
- Right to get their data deleted – “The right to be forgotten”
- Right to restrict and resist use of their data
- Right to move data from one database to the other
- Right to receive information of personal data use violations
- Right to object to use of their data
- Right to not be subject of automated decision making

As a part of the Individuals’ rights is that the data may only be saved for a period of 12 months after the expiration of contract or only 3 months after when there is no longer a vital interest to save the data. Personal data for marketing can only be kept for 3 months. If a consent is withdrawn personal data must be deleted within 30 days.

Consent for the use of personal data must be collected for every purpose the organisation is using the personal data for

For Sport Organisations who buy services from outside providers for membership databases, accreditation tools or result services, it is imperative to renegotiate your deals with them, so that they also are in line with the new GDPR, as you as the owner of the data are responsible for it.

It is important to keep in mind the basic principle that only essential data should be saved and not think this information “might be useful”!

4) Risk Assessment

The GDPR gives the organisations the task to evaluate and assess the possible risks that are related to the handling of personal data. Here the risks refer to the situations where the individual may face physical, material or immaterial damage, for example when improper processing of the personal data may lead to segregation, identity theft or fraud. The registrant and processor of the personal data must to all means possible act in order to minimize these risks.

5) Contracts when providing personal data to outside operators

The right to provide personal data to an outside operator, must be based on one of the reasons mentioned in point 2) and the fact that the data has been provided must be informed to the person in question. In the contract, based on which the data is provided to the outside operator, there must be define the source of persons, the reason and the time-line for the use of the data, the type of personal data and the contractor must agree to the following obligations:

1) To process the personal data only in accordance with documented instructions of the registrant
2) To follow the principle of non-disclosure in the process
3) To follow all needed security measures for the use of Sensitive Personal Data
4) That all processing the personal data are following the same rules as what has been defined contract between the registrant and the individual.

5) To help the registrant with technical and organisational measures to make changes in the data, if required by the individual
6) To delete or return all personal data after the contract ends to the registrant and to delete all copies of the databases

It is imperative to check which of all outside services might be affected here.

6 The obligation to inform about data protection breaches

The registrant is obliged to inform about any data protection breaches to the person in question and the data protection officials. A data breach includes the involuntary or illegal destruction of data, changing of data, unauthorised surrendering of data or providing access to the data. The registrant shall inform the data protection officials, as far as possible within 72 hours from when the data protection breach has happened. The information to the data protection officials can only be neglected if the data breach has only a minor risk to the individuals' rights and freedom.

The registrant needs to document all data breaches of the personal data, including all details of when and where the breach has occurred, what effect has it has had and the corrective measures.

As a part of the usage of the personal data, it would be important to make a plan for possible data breaches, in order to identify the possible threat, informing about them, to clear up the situation and to document the incident and update guidelines for further use of personal data.

7 Data protection officer

An organisation must define a person responsible for data protection, if their key activities are related to the use of personal data in a larger scale. This is still to be defined when it relates to sport organisations.

It is likely that the sport organisations will need to name a Data protection officer, if they are keeping athletes' databases or similar lists on persons. The Data protection officer can be a person in the organisation or an outside service.

What to do!

Please look over the following issues:

- Clarify what personal data is being gathered and processed and if they are collocated into a database
- Clarify on which basis the personal data is collected and processed and if they are surrendered to outside organisations
- Make a list of all different data bases of individuals and make a register document of these.
- How have your organisation secured data protection and risk assessment and minimizing?
- Is a Data protection officer needed? Name this if needed
- How do you secure the rights of the Individuals', named in point 3.
- How to act in case of a data protection breach.

- How to include the requirements for providing personal data to third parties in contracts

Carefully document all these points into a Data protection document and educate your employees and volunteers in the field of data protection.