GAISF

One Voice for all Sport

GDPR

THE NEW DATA PROTECTION REGULATION

GAISF
One Voice for all Sport

1. Data inventory

List all categories of data subjects.
E.g. : Personal data of our members / applicants / employees / consultants / providers / athletes videos and pictures / Registrars /registrants /…

For each category

- Type of data collected
  - Professional life
  - Personal life
  - Economic and financial
  - Online browsing history
  - Religious, philosophical, …
  - …
- Source of data
  - Direct from data subject
  - Indirect, from data processor

GAISF
One Voice for all Sport

1. Data inventory (Ctd’)

- Processing purpose
  - Your objectives when processing data (service enhancement, marketing, HR, research, ..)
- Legal basis for processing
  - Elect one or many of the 6 legal basis
- Retention period
- Storage location
  - Cloud /cloud locations
  - Physical server
  - Personal computers
  - Phones
- Who has access internally
- Who has access externally

GAISF
One Voice for all Sport

2. Questionnaire

Various questionnaires available – we based ours on DPCI (Data Protection Commissioner of Ireland) form.
It is devided in 8 chapters :

1. Personal Data
2. Data subjects rights
3. Accuracy and retention
4. Transparency requirements
5. Other Data Controler obligations
6. Data Security
7. Data breaches
8. International Data transfer

GAISF
One Voice for all Sport

Personal data

PERSONAL DATA	Question	Yes	No	Comment / remedial action
Consent based data processing (Articles 7, 8 and 9)	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of statement or a clear affirmative action?			
	If personal data that you currently hold on the basis of consent does not meet the required standard under the GDPR, have you re-sought the individual's consent to ensure compliance with the GDPR?			
	Are procedures in place to demonstrate that an individual has consented to their data being processed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
Children's personal data (Article 8)	Where online services are provided to a child, are procedures in place to verify age and get consent of a parent/ legal guardian, where required?			
Legitimate interest based data processing	If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? That analysis must demonstrate that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, and 3) the processing is not prejudicial to or overridden by the rights of the individual.			

GAISF
One Voice for all Sport

Data subject rights

DATA SUBJECT RIGHTS				
Access to personal data (Article 15)	Is there a documented policy/procedure for handling Subject Access Requests (SARs)?			
	Is your organisation able to respond to SARs within one month?			
	Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format?			
	Are there controls and procedures in place to allow personal data to be deleted or rectified ?			
	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing ?			
	Are individuals told about their right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest?			
	Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
Restrictions to data subject rights (Article 23)	Have the circumstances been documented in which an individual's data protection rights may be lawfully restricted?			

GAISF
One Voice for all Sport

Accuray and retention

ACCURACY AND RETENTION				
Purpose limitation	Is personal data only used for the purposes for which it was originally collected?			
Data minimisation	Is the personal data collected limited to what is necessary for the purposes for which it is processed?			
Accuracy	Are procedures in place to ensure personal data is kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Retention	Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected?			
Other legal obligations governing retention	Is your business subject to other rules that require a minimum retention period (e.g. medical records/tax records)?			
	Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies?			
Duplication of records	Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records?			

GAISF
One Voice for all Sport

Transparency requirements

Transparency to customers and employees (Articles 12, 13 and 14)	Are service users/employees fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form using clear and plain language?			
	Where personal data is collected directly from the individuals, are procedures in place to provide the information listed at Article 13 of the GDPR?			
	If personal data is not collected from the subject but from a third party (e.g. acquired as part of a merger) are procedures in place to provide the information listed at Article 14 of the GDPR?			
	When engaging with individuals, such as when providing a service, sale of a good or CCTV monitoring, are procedures in place to proactively inform individuals of their GDPR rights?			
	Is information on how the organisation facilitates individuals exercising their GDPR rights published in an easily accessible and readable format?			

GAISF
One Voice for all Sport

Other Data Controller obligations

OTHER DATA CONTROLLER OBLIGATIONS				
Supplier Agreements (Articles 27 to 29)	Have agreements with suppliers and other third parties processing personal data on your behalf been reviewed to ensure all appropriatedata protection requirementsare included?			
Data Protection Officers (DPOs) (Articles 37 to 39)	Do you need to appoint a DPO as per Article 37 of the GDPR?			
	If it is decided that a DPO is not required, have you documented the reasons why?			
	Where a DPO is appointed, are escalation and reporting lines in place? Are these procedures documented?			
	Have you published the contact details of your DPO to facilitate your customers/ employees in making contact with them? (Note: post 25 May 2018 you will also be required to notify your data protection authority of your DPO's contact details)			
Data Protection Impact Assessments(DPIAs) (Article 35)	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			

GAISF
One Voice for all Sport

Data security

DATA SECURITY				
Appropriate technical and organisational security measures (Article 32)	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
	Is there a documented security programme that specifies the technical, administrativeand physical safeguards for personal data?			
	Is there a documented process for resolving security related complaints and issues?			
	Is there a designated individual who is responsible for preventing and investigating security breaches?			
	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
	Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained.			
	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			

Data breaches

DATA BREACHES				
Data Breach response obligations (Article 33 and 34)	Does the organisation have a documented privacy and security incident response plan?			
	Are plans and procedures regularly reviewed?			
	Are there procedures in place to notify the office of the Data Protection Commissionerof a data breach?			
	Are there procedures in place to notify data subjects of a data breach (where applicable)?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, suppliers and other partners to deal with data breaches?			

GAISF
One Voice for all Sport

International data transfer

INTERNATIONAL DATA TRANSFER (OUTSIDE EEA) - IF APPLICABLE				
International data transfers (Articles 44 to 50)	Is personal data transferred outside the EEA, e.g. to the US or other countries?			
	Does this include any special categories of personal data?			
	What is the purpose(s) of the transfer?			
	Who is the transfer to?			
	Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is?)			
Legality of international transfers	Is there a legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses. Are these bases documented?			
Transparency	Are data subjects fully informed about any intended international transfers of their personal data?			

GAISF
One Voice for all Sport

3. Iterative process

Answers elaborated and collected by one person inside your organisation
Ideally, shared with a third party expert for feedback and suggested measures to take
Take apropriates measures from an

- IT perspective
- Legal perspective
- Process perspective

GAISF
One Voice for all Sport

Next workshops

- IT perspectives
  - 3 IT experts will go guide you through the IT answers to GDPR requirements
- Legal perspectives
  - 2 specialised lawyers will bring you

Http://www.gdpr.sport

GAISF
One Voice for all Sport

Questions