

## **IPACS Benchmark Guidelines**

**Updated 5 November 2021**

### **IPACS Benchmark B8 – The organisation is compliant with applicable laws regarding data protection and takes measures to ensure IT security**

#### Definitions

- Data protection laws – the legislation applicable to data protection that is in place in particular jurisdictions, such as General Data Protection Regulation in the European Union and the application of the Council of Europe Convention 108
- IT security – mitigating the risks for computer systems and information relating to accidental or unauthorised access, disclosure, modification, disruption, loss, use or deletion of data

#### Introduction to this Benchmark and its significance

- Sports organisations must comply with the law, even if this requires significant modification to previous practices that were carried out before specific legislation was enacted
- Along with other sectors, sports organisations need to protect individuals' personal data and against ongoing threats to IT security
- Demonstrating a competent and responsible approach to data protection and IT security and compliance with the applicable legal frameworks can help increase trust in the organisation among stakeholders, both internally and externally

#### Commentary on the action to be taken

- The organisation should ensure that it complies with the applicable laws regarding data protection and IT security; in the case of an organisation which is international in scope, multiple laws may apply, international treaties (such as the Council of Europe Convention 108) could be a point of reference for multi-jurisdictional cases
- Related policies should be made available, and where appropriate published on the website
- Data protection should be supported by design and by default approaches
- Recommendations from reviews and audits of IT security should be acted upon

Investment requirement – some initial investment is required to ensure procedures are compliant and to mitigate risks; the ongoing need for investment may be more limited

#### Guidance according to stage of organisation

##### Early stage

- The organisation maps the data processing it undertakes, applies privacy by design and conducts a privacy impact assessment where needed, drawing up a risk mitigating strategy
- The organisation publishes a basic privacy policy on its website

##### Developing

- The organisation's policies are published and compliance with applicable data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, is ensured
- The organisation conducts regular reviews of IT security measures

##### Advanced

- The organisation conducts additional activities in relation to data protection and IT security, such as training for staff/officials
- The organisation takes action following reviews or audits to mitigate risks identified

## Good practice examples

### International Federations (from June 2020)

- ITU: A variety of policies relating to [GDPR](#) are published [https://www.triathlon.org/privacy\\_notice](https://www.triathlon.org/privacy_notice)
- FIFA: [FIFA Data Protection Regulations](#) are issued and applicable to all member associations, as well as their members  
FIFA held a [Data Protection Summit](#) for a wide range of stakeholders
- UCI: UCI staff are regularly informed of risks and best practices in relation to data protection and IT security. Security measures are in place and the UCI ensures that relevant rules are complied with by contracting partners. GDPR is referenced in the [Data Protection Policy](#)

### Overall standard among International Federations:

- 26 out of 31 ASOIF members had published a form of privacy policy or data protection policy on its website

### Continental Bodies

- European Olympic Committees: [Privacy policy](#) published

### National Olympic Committees

- British Olympic Association: [Privacy policy](#) published
- Korean Sport and Olympic Committee: [Open data procedure](#)
- Indian Olympic Association: [Document retention policy](#)

### National Federation

- Sportbund Rheinland, Germany: [GDPR guidance for sport organisations in Germany](#)

### Selected references

- [ASOIF GTF Questionnaire 2019-20](#), Indicator 3.10
- European Commission Expert Group on Good Governance, “Principles of Good Governance in Sport”:
  - Principle 10.c: Internal control measures
  - “Sports bodies should adopt proportionate, fit for purpose internal controls, reporting requirements, data protection policies and financial management strategies to at least the level required by applicable laws. Such policies should include clear financial authorisation limits and formalisation of agreements in legally enforceable form”
- [Council of Europe Data Protection Website](#) – Convention 108
- [Overview of data protection laws around the world](#)
- [European Union General Data Protection Regulation](#)
- Brazil - [General Law for the Protection of Personal Data](#)
- [Council of Europe Convention on the Manipulation of Sports Competitions](#) (2014) – Articles 12 to 14 on exchanging information and data protection

### ASOIF indicator 3.10 – scoring definitions used in the 2019-20 assessment

- 0 – No
- 1 – Some evidence of action taken regarding data protection issues
- 2 – IF is compliant with applicable data protection laws, such as GDPR, and undertakes IT security measures
- 3 – IF is compliant with applicable data protection laws and provides training for staff members, undertakes regular risk reviews of its security of IT systems with actions taken to mitigate risks
- 4 – State of the art policies and procedures in place