world anti-doping agency

Privacy and Data Protection

Professional Standard

GLDF | Global **L**earning and **D**evelopment **F**ramework

The professional standard aims to support the anti-doping industry by providing a benchmark of competence for a specific role. Anti-Doping Organizations (ADOs) can use the professional standard to support the evaluation of competence and importantly to support practitioner development by identifying professional development needs

The professional standard:

- describes the main functions for a given anti-doping role
- details the expected standard of competence for each of these functions (using performance criteria)
- details the knowledge and skill requirements for the role

Version: 1.1
Published: January 2024

KEY PURPOSE

Assist the anti-doping organization in maintaining accountability and trust in its handling of personal information by implementing privacy and data protection standards and fostering a privacy and data protection culture in the organization

Main functions

Develop and implement a privacy and data protection program to protect personal information from unauthorized use or other compromise

- **1.1.** Contribute to the development of a governance structure for the privacy and data protection program
- **1.2.** Develop, monitor, and maintain a comprehensive understanding of the data that the organization stores and processes
- **1.3** Develop internal privacy and data protection policies, procedures and protocols, and support and monitor their implementation
- **1.4.** Develop external privacy policies and notices and communicate them to relevant stakeholders
- **1.5.** Develop and test a plan to respond to potential privacy and data incidents

Foster a privacy and data protection culture within the organization

- **2.1.** Promote awareness of privacy and data protection requirements and support staff in their implementation
- **2.2.** Develop and provide privacy and data protection training to the organization's staff

Provide support, advice, and information to help the organization manage risks tied to the processing of personal information

- **3.1.** Identify applicable privacy and data protection legal requirements
- **3.2.** Support the identification of privacy and data protection risks in the organization's processing activities
- **3.3.** Coordinate the organization's response to privacy and data incidents
- **3.4.** Process and respond to requests and complaints from data subjects about personal information rights
- **3.5.** Process and respond to enquiries and investigations from regulatory authorities
- **3.6.** Assess third party agent risks to ensure appropriate controls and measures to mitigate risk are in place

1 Develop and implement a privacy and data protection program designed to protect personal information from unauthorized use or other compromise

	Performance Criteria You must be able to:	Knowledge and understanding
1.1 Contribute to the development of a governance structure for the privacy and data protection program	PC1 Identify the decision-making person or body of the organization that is ultimately accountable for privacy and data protection PC2 Outline how responsibility for privacy and data protection matters are delegated within the organization to the privacy and data protection function PC3 Establish how the privacy and data protection function is expected to report up to this decision-making person or body PC4 Identify roles in the organization that are complementary to, or closely linked to the privacy and data protection function and establish cross-functional collaborative mechanisms PC5 Assess and establish respective responsibilities, reporting structure and working relationships appropriate to the organization PC6 Document the governance framework that supports the privacy and data protection program PC7 Review the governance structure and suggest improvements on a regular basis	K1 Overall governance structure of the organization K2 Organizational structure as related to strategy, operations and management for responsibilities and reporting K3 Each major department/unit's functions and responsibilities K4 Expectations and/or requirements regarding governance, privacy and data protection function, and organizational structure in applicable privacy and data protection standards

1.2 Develop, monitor, and maintain a comprehensive understanding of the data that the organization stores and processes	PC1 Choose a format or tool that you will use to record processing activities that suits your capacities and that covers the minimum information that you must include in your record under applicable standards PC2 Identify the activities of your organization that involve personal information, including collection, processing, and disclosure of data PC3 Record, for each activity, what types of personal information are collected, how they are used, who they are shared with, and how long they are retained PC4 Record, where information is shared, the safeguards that are in place to ensure the information is protected PC5 Record, for each activity, the systems, applications, and software used to process the information PC6 Regularly review records to ensure new, or changes to existing activities of your organization that involve personal information are included	K1 The minimum information that you must include in the record for each processing activity, under applicable standards K2 What personal information is and a general awareness of the types of organizational activities that involve processing of personal information K3 Formats and tools that can be used to record processing activities and how to select ones appropriate to your organization K4 How different types of data are categorized K5 Retention periods for personal information under applicable standards and organizational policies K6 Types of safeguards that are in place to ensure the information is protected and how these affect privacy and data protection
1.3 Develop internal privacy and data protection policies, procedures and protocols, and support and monitor their implementation	PC1 Map your organization's responsibilities under applicable privacy and data protection standards PC2 Develop and maintain policies, procedures and protocols that meet applicable organizational responsibilities and address privacy and data protection risks PC3 Develop procedures or protocols to ensure appropriate safeguards to are in place when information is shared PC4 Communicate policies, procedures and protocols to relevant internal stakeholders and support their implementation PC5 Monitor or assign responsibilities for monitoring the implementation of policies, procedures, and protocols	K1 How to develop policies, procedures, and protocols K2 General awareness of typical privacy and data protection policies, procedures, and protocols K3 Types of safeguards to ensure the information is protected when shared K4 General awareness of monitoring procedures and practices

1.4 Develop external privacy policies/ notices and communicate them to relevant stakeholders	PC1 Develop appropriate external privacy policies/notices, using clear and plain language, explaining your data processing activities and related information, as well as data subjects' privacy and data protection rights and choices, in line with applicable requirements PC2 Communicate the external privacy policies/notices to data subjects within applicable timelines PC3 Obtain valid consent for the collection and processing of information when you need it	K1 Data flows and points of interactions with data subjects K2 Required content and timelines for providing privacy notices to data subjects under applicable standards K3 When and how you need to obtain valid consent from data subjects K4 Data subjects' privacy and data protection rights and choices
1.5 Develop and test a plan to respond to potential privacy and data incidents	PC1 Document responsibilities for incident response in a response plan, across the five key steps of discovery, containment, assessment, notification, and remediation PC2 Identify responsible individuals for each of the key response areas PC3 Liaise with the relevant stakeholders to ensure there is an escalation process and a determination of when the responsible individuals for incident response need to be involved PC4 Review applicable standards and layer in or adapt each of the incident response steps according to applicable standards PC5 Ensure your plan includes the identity, role and contact information of external third parties that you would be in contact with, if any, in the event of an incident PC6 Ensure your staff are instructed on how to respond promptly to an incident PC7 Conduct periodic testing of your plan to identify and address the improvements to be made PC8 Maintain a breach notification and reporting protocol	K1 The types of privacy and data incidents which may occur K2 Key privacy and data incident response steps (discovery, containment, assessment, notification, and remediation) and their respective requirements K3 The types of third parties that may need to be involved in a privacy and data incident response K4 How to set up and implement periodic testing of a plan to respond to privacy and data incidents K5 Breach notification and reporting protocols in your organization

2 Foster a privacy and data protection culture within the organization

	Performance Criteria You must be able to:	Knowledge and understanding
2.1 Promote the awareness of privacy and data protection requirements and support staff in their implementation	PC1 Gain consensus from members of the organization's management on privacy and data protection as an imperative PC2 Develop internal tools and resources or identify existing ones that facilitate compliance with privacy and data protection policies, procedures, and protocols and make them available to relevant colleagues PC3 Educate staff about the importance of balance between privacy and data protection requirements and organizational needs regarding data, thereby cultivating an understanding of privacy and data protection requirements as integral to organizational activities	K1 Internal privacy and data protection policies, procedures, and protocols K2 How to identify tools and resources that may be useful to organizational staff K3 Frequently encountered privacy and data protection issues in an anti-doping context K4 The importance of management's buy-in for privacy and data protection matters and how to foster it K5 The importance of staff's perception of privacy and data protection as an asset to organization's operations, and not a barrier
2.2 Develop and provide privacy and data protection training to the organization's staff	PC1 Identify and analyze privacy and data protection knowledge gaps and training needs among the organization's staff PC2 Identify existing internal or external privacy and data protection training resources aligned with the training needs analysis, and develop new resources where needed, including by partnering with internal education managers and Human Resources staff PC3 Ensure that staff have received privacy and data protection training, including with respect to the use of relevant IT platforms such as ADAMS PC4 Customize privacy and data protection training to staff's respective roles where possible PC5 Document the activities undertaken and measure the impact of training efforts over time	K1 How the use of ADAMS's features impacts privacy and data protection K2 Requirements on training contained in applicable standards, including the agreement governing the use of ADAMS K3 How to conduct a privacy and data protection training needs analysis among internal staff K4 General awareness of existing privacy and data protection training resources K5 The importance and benefit of partnering with internal functions to develop privacy and data protection training K6 How to develop role-based privacy and data protection training in alignment with a training needs analysis

3 Provide support, advice, and information to help the organization manage risks tied to the processing of personal information

	Performance Criteria You must be able to:	Knowledge and understanding
3.1 Identify applicable privacy and data protection legal requirements	PC1 Identify the relevant privacy and data protection standards that apply to the activities of your organization PC2 Identify and manage the interplay in applicable privacy and data protection standards PC3 Identify relevant sports and anti-doping laws and evaluate how they interact with privacy, data protection and information security standards PC4 Seek competent opinions, where necessary, regarding developments in privacy and data protection standards PC5 Ensure you stay informed of new developments	K1 The International Standard for the Protection of Privacy and Personal Information (ISPPPI) and associated Guidelines K2 General awareness of global/international privacy and data protection standards K3 How relevant sports and anti-doping laws interact with privacy, data protection and information security standards K4 How to search for and stay informed of new developments regarding privacy and data protection standards K5 How to know what standards apply to your organization K6 The types of interplay that may occur in privacy and protection standards and how to manage these K7 Sources of competent advice on developments in privacy and data protection standards, how to evaluate and access these

✓ 3.2 Support the identification of privacy and data protection risks with the processing activities of the organization	PC1 Liaise with relevant colleagues to capture how personal information is protected and determine if, and which measures should be taken to increase protection PC2 Assess and record if the processing activities meet the organization's responsibilities under applicable privacy and data protection standards and determine which measures, if any, should be taken to ensure compliance PC3 Explain legal requirements under privacy and data protection standards to staff in a manner appropriate to their understanding, needs, situation and operations PC4 Conduct and/or support risk/impact assessments when necessary for the processing of personal information PC5 Record the assessments and the policies, procedures, protocols and controls the organization needs to take to mitigate identified risks, and assign responsibilities PC6 Ensure new, or changes to existing organisational activities that involve personal information undergo appropriate assessment processes	K1 Types of physical, technical, and organizational controls K2 General awareness of information security risks and mitigation measures K3 How to audit compliance of processing activities with applicable privacy and data protection standards K4 General awareness of risk assessment processes for privacy and data protection K5 Mandatory risk/impact assessments to be conducted under applicable standards K6 How to adapt legal advice given in a manner appropriate to the understanding, needs and situation of anti-doping staff K7 How to implement legal requirements in daily anti-doping operations

3.3 Coordinate the organization's response to privacy and data incidents	PC1 Gather all relevant available information regarding the incident PC2 Assess the incident to understand its nature, scope, impact, and severity PC3 Determine whether notification obligations are triggered and adhere to applicable notification timelines PC4 Ensure the appropriate containment and remediation requirements are implemented PC5 Maintain appropriate records regarding the incident, including the facts related to the incident, its effects, your assessment of the incident, and remedial actions taken PC6 Take stock, with the response team, of the failures or gaps that led to the incident, the positive and the negative aspects of your response, and the lessons learned throughout the process, to improve how you manage any future incidents PC7 Document these lessons and update your incident response plan as needed	K1 How to assess the nature, scope, impact, and severity of a privacy and data incident K2 Notification obligations, triggers and timelines K3 The records that need to be kept regarding privacy and data incidents, what they should contain, how long they must be kept, and why record keeping is important K4 How to investigate and identify causes of privacy and data incidents K5 How to evaluate the effectiveness of the response to privacy and data incidents

✔ 3.4 Process and respond to requests and complaints from data subjects about personal information rights	PC1 Document and record personal information rights requests and complaints and acknowledge receipt PC2 Verify the identity of the requester using the minimal amount of personal information required, and, as applicable, the mandate of any third-party representative PC3 Assess the nature and scope of the personal information rights requests and complaints PC4 Request and gather any information needed, with internal and external stakeholders, to respond to the personal information rights requests and complaints, as necessary PC5 Provide a response to the personal information rights requests and complaints within applicable timelines, including required information while applying any exceptions under applicable standards PC6 Ensure that staff, especially staff with frequent interactions with athletes and others, are aware of the possibility that they may receive requests or complaints and are trained to direct these to the privacy and data protection function. PC7 Escalate any unresolved complaints following agreed procedures	K1 The importance of responding to requests and complaints according to required standards K2 Individual rights regarding personal information under applicable standards and exceptions K3 The ADO's role with respect to the personal information that is the subject of the request/ complaint K4 Good practices on how to verify and confirm the identity and mandate of a requester K5 Which staff are most likely to receive requests and complaints K6 Escalation procedures for complaints from data subjects
✔ 3.5 Process and respond to enquiries and investigations from regulatory authorities	PC1 Inform the decision-making person or body of the organization that is ultimately accountable for privacy and data protection of the enquiry and investigation and its scope PC2 Organize and gather the needed elements to respond, including obtaining required information from third parties, as applicable. PC3 Ensure prompt communication & collaboration with the regulatory authority	K1 Governance structure of the privacy and data protection program K2 The importance and stakes of collaborating with regulatory authorities K3 Best practices for cooperation with regulatory authorities

⚠ 3.6 Assess third party agent risks to ensure appropriate controls and measures to mitigate risk are in place	PC1 Evaluate the type of third-party agent, the nature and scope of the third-party agent's services and legitimate needs with respect to the processing of personal information PC2 Conduct risk assessment of third-party agent prior to agreeing to their processing of personal information and identify controls and measures to mitigate risks PC3 Subject third-party agents to the organization's privacy and data protection requirements and appropriate controls to protect personal information that will be in their custody PC4 Document the arrangement with the third-party agent in an agreement that complies with applicable standards PC5 Tailor access permissions of third parties in any systems in a manner that respects the principles of data minimization and need-to-know PC6 Review long-term third-party agent agreements for new or evolving privacy and data protection risks	K1 Types of third-party agents in the anti-doping context and the respective requirements regarding their processing of personal information under applicable standards K2 Appropriate controls to implement for third-party agents' processing of personal information, including mandatory ones under applicable standards K3 General awareness of information security risks and mitigation measures K4 How to assess third party agent risk K5 How to tailor access permissions in ADAMS

Glossary

Applicable privacy and data protection standards (or applicable standards):

Any privacy and data protection standard that may apply to the operations of the relevant anti-doping organization, including the World Anti-Doping Code, the International Standard for the Protection of Privacy and Personal Information (ISPPPI) and associated Guidelines, the organizational specifications, and/or regional and national laws and regulations.

Skills

Based on the results of a survey that was circulated among privacy and data protection practitioners across the anti-doping industry in 2021, a list of skills was identified as necessary for the profession. The following list details skills deemed as essential by over 65% of respondents. Such skills should be assessed in candidates applying for a privacy and data protection role:

- Ability to work in compliance with code, standards, ethics
- Ability to work with sensitive information and maintain confidentiality
- Writing
- Listening
- Analytical and logical thinking
- Decision making
- Planning
- Project management
- Attention to detail
- Speaking
- Goal setting
- Ability to develop, write and edit legal documents
- Critical thinking
- Risk analysis
- Being able to use word processing spreadsheets, social media, data visualization and email communication
- Strategic thinking
- Ability to lead change
- Ability to give and receive feedback
- Teamwork collaboration
- Self-motivation
- Stress management
- Willingness and ability to learn

Collaborators

WADA, while leading the standard setting work to develop the professional standards, works collaboratively with stakeholders and WADA technical teams. The development work for Privacy and Data Protection was conducted by the Technical Working Group composed of:

- **Daniel Cooper** - Covington & Burling LLP
- **Frederique Horwood** - WADA
- **Johanna Szymczak** - NADA Germany
- **Julia Hardy** - UKAD
- **Nicholas Shepherd** - Covington & Burling LLP
- **Rachel Campbell** - Osler Hoskin & Harcourt
- **Regine Reiser** - NADA Germany

This group was chaired by an Education practitioner from the anti-doping industry:

- **Katrien Daelman** - WADA

Quality Management

Version: **1.1**
Endorsed by: WADA Education Committee
Endorsement date: November 2021
Publication date: January 2024

GLDF Overview

One of WADA's six priorities under the World Anti-Doping Agency's 2020-2024 Strategic Plan is to 'Grow Impact'. As one of the key initiatives under this priority, the Agency has committed 'to developing training programs and qualifications standards for anti-doping professionals to improve professionalism and enhance the capabilities of the anti-doping workforce'.

Accordingly, in April 2020, WADA's Education Department commenced development of a Global Learning and Development Framework (GLDF), through which specific, standardized training for a range of anti-doping roles are being developed and made available for Anti-Doping Organizations (ADOs) and other stakeholders worldwide within the anti-doping ecosystem. The GLDF establishes role descriptors, professional standards and global learning and development activities for practitioner roles in the anti-doping industry.
The professional standards have been used by WADA to develop competency-based training programs. They can be read alongside:

(1) the role descriptor for the corresponding role, a simple document which clarifies the main characteristics of key anti-doping roles and can be used as a basis for developing a job description when ADOs are looking to recruit a position for a given role.

(2) the anti-doping core competency framework, which details the values and competencies that are common across the various roles in the anti-doping industry.

*** The Professional (occupational) Standards are the benchmarks of good practice and describe the expected standard of competence for a given role. They should not be confused with the International Standards, which are a set of documents that, along with the World Anti-Doping Code, seek to harmonize anti-doping policies, rules and regulations among Anti-Doping Organizations (ADOs) for specific technical and operational parts of anti-doping programs.***

world anti-doping agency