



2021 Code Implementation Support Program
Guidelines for the International
Standard for the Protection of Privacy
and Personal Information

GUIDELINES FOR PRIVACY

Contents

GUIDELINES FOR PRIVACY	2
WELCOME TO THE GUIDELINES FOR PRIVACY	4
Introduction.....	4
Context	4
Beyond the ISPPPI	4
How to use the Guidelines	5
SUMMARY	6
HOW TO MAKE PRIVACY A PRIORITY	9
1. Ensuring privacy is part of your organization’s key objectives	9
2. Creating a privacy role, team or department	10
THE FOUNDATIONS OF YOUR PRIVACY PROGRAM	13
1. Understanding fair information principles	13
2. Understanding the ISPPPI's place in your privacy program.....	15
3. Integrating privacy and data protection laws	16
HOW TO STRUCTURE YOUR PRIVACY PROGRAM	19
1. Identifying your governance structure	19
2. Assigning roles and responsibilities.....	20
3. Defining requirements that the organization must meet.....	20
4. Writing it down and making it mandatory	21
HOW TO IDENTIFY WHAT YOU HOLD AND WHY	23
1. Creating a record of processing	23
2. Identifying the facts.....	25
3. Applying ISPPPI requirements	27
4. Assessing and mitigating risks	30
HOW TO EXPLAIN YOUR PROCESSING PRACTICES	32
1. Preparing a privacy notice	32
2. Providing your privacy notice to the right people, at the right time, in the right way	35

3.	Obtaining valid consent if you need it.....	37
	HOW TO PROTECT PERSONAL INFORMATION	40
1.	Building and implementing an information security program	40
2.	Implementing appropriate security safeguards	42
	HOW TO PREPARE FOR AND RESPOND TO A BREACH	46
1.	Creating a response plan	46
2.	Testing your plan	50
3.	Responding to a breach	50
	HOW TO SHARE PERSONAL INFORMATION RESPONSIBLY	53
1.	Identifying and classifying third parties.....	54
2.	Applying common principles.....	55
3.	Sharing with other ADOs	56
4.	Sharing with third-party agents.....	58
5.	Sharing with Other Third Parties	62
	WHAT PERSONAL INFORMATION SHOULD BE RETAINED	65
1.	Understanding Annex A of the ISPPPI.....	65
2.	Implementing Annex A outside of ADAMS	66
3.	Defining retention periods for other data	68
4.	Deleting, destroying or anonymizing when retention periods expire.....	68
	HOW TO RESPOND TO REQUESTS AND COMPLAINTS	70
1.	Understanding individual rights regarding personal information	70
2.	Responding to a request or complaint.....	72
	HOW TO CREATE A PRIVACY CULTURE.....	79
1.	Training your privacy champions.....	79
2.	Training your staff & raising awareness	80

Welcome to the Guidelines for Privacy

Introduction

Welcome to the Guidelines for Privacy (Guidelines), a third-level, non-mandatory document that supports the International Standard for the Protection of Privacy and Personal Information (ISPPPI). These Guidelines aim to better equip Anti-Doping Organizations (ADOs) in applying appropriate and effective privacy protections, as described in the ISPPPI.

Where the ISPPPI sets forth a minimum of what to do, these Guidelines aim to help you understand how to do it, giving you examples and suggestions, and showing you how to go above and beyond where possible.

Context

Under the World Anti-Doping Code (Code), ADOs commit to protecting and lawfully processing personal information in connection with their anti-doping activities. This is essential to ensure the continued confidence and trust of athletes and other individuals who are subject to anti-doping rules.

With the ISPPPI and the Guidelines, ADOs can develop privacy programs that enhance trust by helping athletes understand how their personal information is handled and protected at each step of the anti-doping process, and by reducing security and privacy risks to personal information.

Beyond the ISPPPI

Most countries around the world have enacted privacy and data protection legislation. In fact, 66% of countries have already done so, and an additional 10% have a draft law¹.

The ISPPPI provides a minimum, common set of standards for the treatment of personal information used in anti-doping activities. It is a foundation upon which ADOs can build a privacy program that also complies with privacy and data protection laws that apply to them.

These Guidelines provide supporting information and guidance to help you build a privacy program that you can tailor to your ADO's needs and context.

¹ United Nations Conference on Trade and Development, Global Cyber Law Tracker (Data Protection and Privacy Legislation Worldwide), <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (last accessed 14 October 2020).

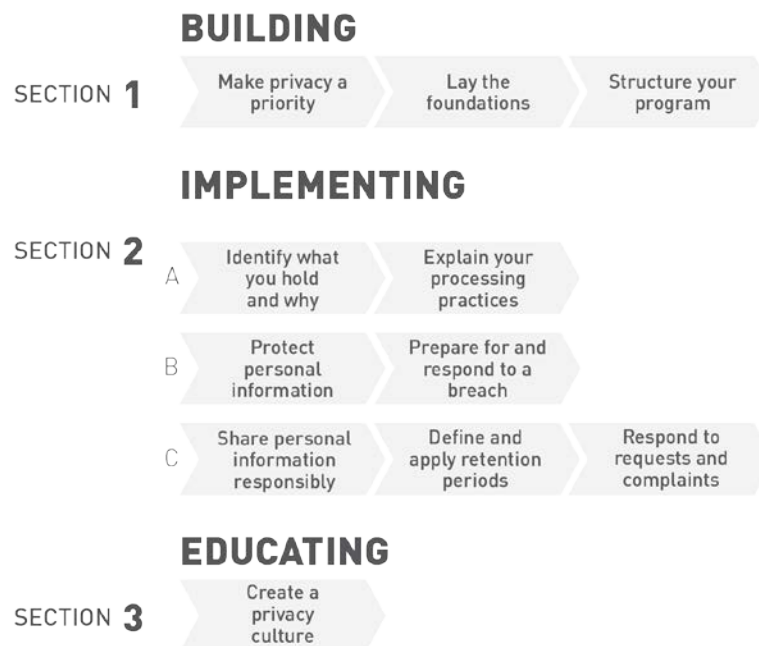
How to use the Guidelines

So, how can you make the most of the Guidelines? The Guidelines are a support tool for all sizes of ADOs, large or small. We understand that different organizations may have different needs, so we have designed the Guidelines in clear sections and chapters to help you navigate through it in a way that works for you. We have also avoided using defined terms and definitions for this latest edition.

If you are new to privacy or anti-doping, or if you are just beginning to develop a privacy program, it might be helpful to read the Guidelines from start to finish and use the examples, figures and templates for your own work. Doing so will lead you through a logical process to develop and implement your privacy program.

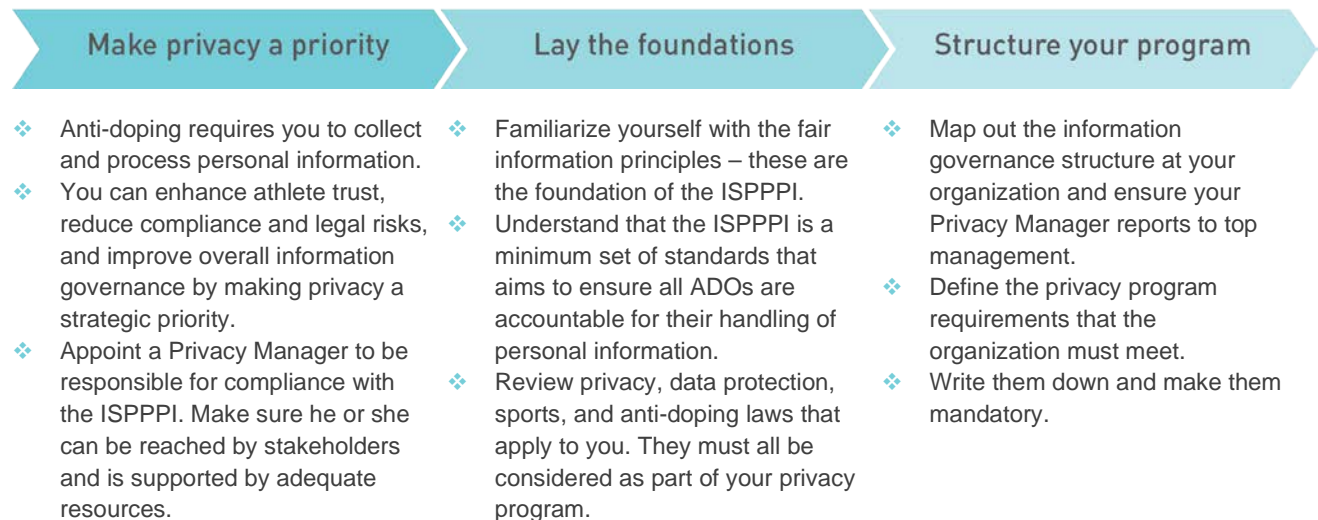
If you are seeking support on a particular item or article from the ISPPPI, select the chapter that suits your needs and go directly to it. If more context is needed, you may want to review other chapters.

If you want an initial snapshot of the contents of the Guidelines, or need a quick refresher or reference guide, consult the summary to identify what chapters will best assist you in your work. And as you build, update or improve your privacy program, remember that in addition to these Guidelines, you can find a suite of ISPPPI resources to help you achieve your goals on [ADEL](#).

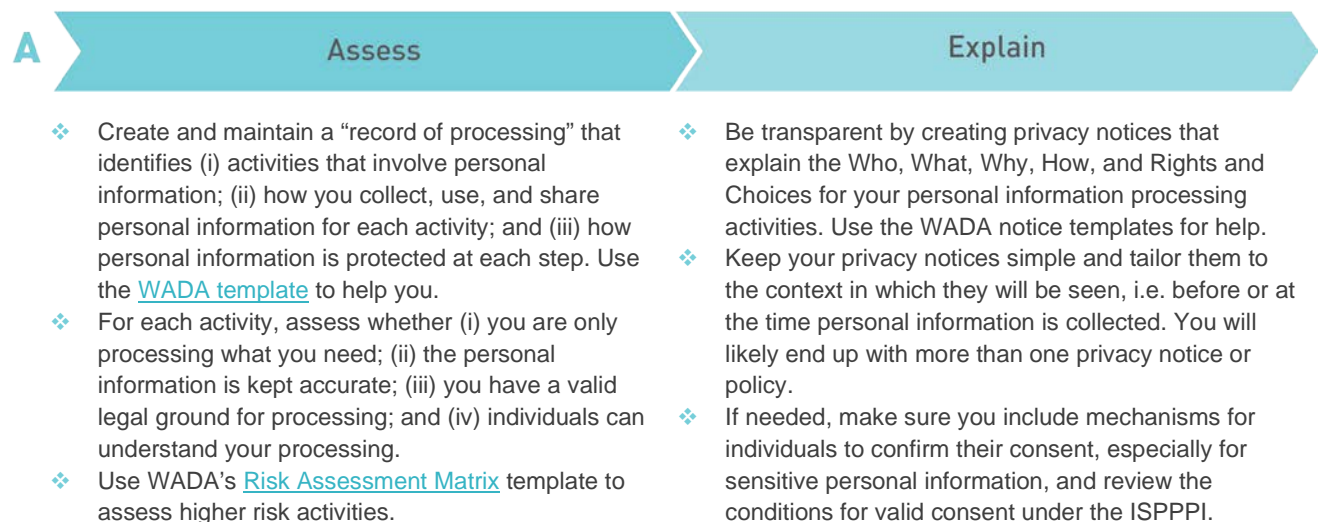


Summary

BUILDING



IMPLEMENTING



B

Protect

- ❖ Establish an information security program to protect personal information. You will need to use a combination of physical, environmental, organizational, and technical measures to protect personal information.
- ❖ Catalog the systems, applications and software you use to process personal information; understand how cyber risks would impact these assets; and assign responsibly for protecting them.

Prepare for & respond to a breach

- ❖ Establish a breach response plan addressing five key steps: discovery, containment, assessment, notification, and remediation. Test it.
- ❖ Assign responsibilities to a breach response team with complementary skills.
- ❖ In the event of a security breach, assess the severity and impact of the breach to determine if you need to notify affected individuals, other organizations, or regulators.
- ❖ Keep appropriate records. Use WADA's [Security Breach Reporting Form](#) or [Log](#) for help.

C

Share responsibly

- ❖ Apply common principles before sharing personal information outside of your organization: (i) identify a need to know; (ii) minimize what is shared; and (iii) use technical and contractual controls to protect the information.
- ❖ Apply additional requirements depending on the type of recipient, whether an ADO, a third-party agent, or another third party. The further removed the third party is from you, the stricter the requirements will be.

Define & apply retention periods

- ❖ Take the time to review and understand Annex A of the ISPPPI. Apply these retention periods in your own systems and to your own records.
- ❖ For data/processing purposes not covered by Annex A, consider what other retention criteria apply, including legal requirements or limitation periods.
- ❖ When personal information is no longer required, it must be deleted, destroyed, or anonymized.

Respond to requests & complaints

- ❖ To respond to requests to exercise rights under the ISPPPI or to a complaint, start by classifying it (e.g. a request to access information, correct or limit processing, or refuse or withdraw consent).
- ❖ Then, acknowledge receipt, gather the information you need to respond, and apply any relevant exceptions (e.g. redacting the personal information of a third party).
- ❖ Make sure your response is timely, reasoned, and understandable for the recipient.

EDUCATING

Create a privacy culture

- ❖ Set yourself the goal of creating a privacy culture, where every person can instinctively apply privacy principles to their day-to-day anti-doping activities.
- ❖ Start by training your privacy champions so they can spread their expertise across the organization. Then, create a privacy training program and make it mandatory to ensure it reaches all staff.
- ❖ The program should cover topics like legal requirements, internal policies, cyber threats, and how to protect personal information. Use ready-made resources or learning management systems for help.
- ❖ Measure progress and reinforce learning with additional training, phishing simulators, and regular awareness reminders.

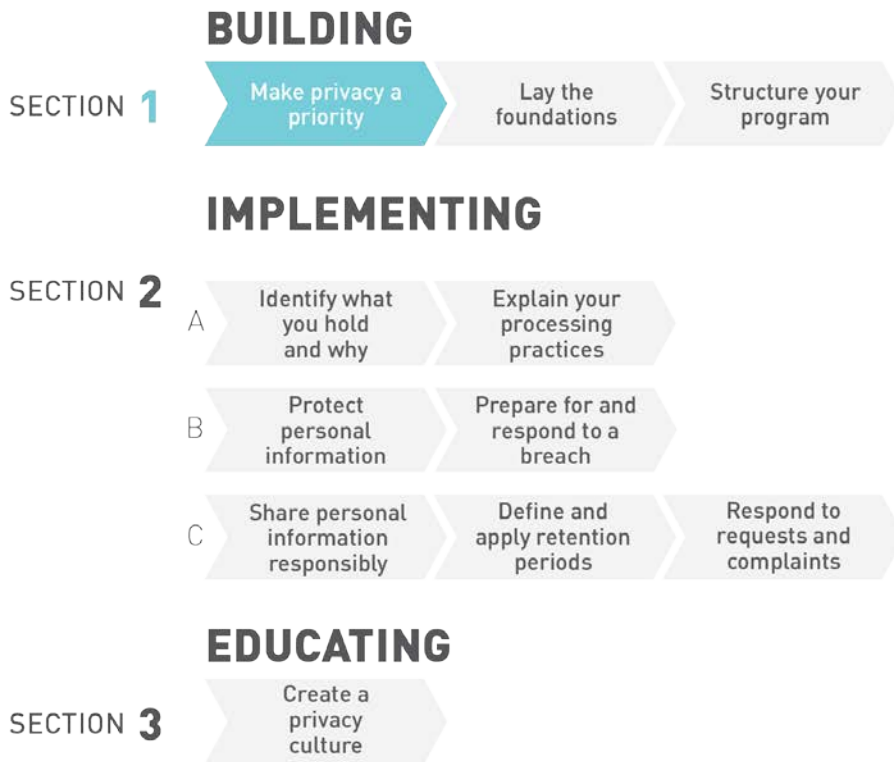
SECTION 1:

Building a privacy program

Section 1 includes Chapters 1, 2 and 3. This section will provide support for Article 4.0 of the ISPPPI – *Processing Personal Information in Accordance with International Standard and Applicable Law* – by helping you make privacy a priority within your organization, understand the key principles of the ISPPPI, build a framework for your privacy program, and identify resources that can support you along the way.



How to make privacy a priority



1. Ensuring privacy is part of your organization's key objectives

Every aspect of anti-doping, from education through to results management, requires athletes to supply some personal information. The Code affirms the importance of ensuring that the privacy rights of individuals subject to anti-doping programs are fully protected. Similarly, the Athletes' Anti-Doping Rights Act provides that athletes have the right to the fair, lawful, and secure handling of their personal information.

To achieve this objective, privacy protections must be built into every anti-doping process. To help you identify whether privacy is adequately prioritized at your organization, consider the following questions:

- ❖ Does your organization have strategic or operational objectives or goals for the future?
- ❖ Does privacy, information management, or information security feature in these priorities?
- ❖ Are there existing or future plans to dedicate human, IT, financial or other resources to privacy protection?

If you answered 'no' to any of the above questions, you will need to work towards making privacy a priority in your organization. To help you do so, consider the following ways better privacy protections will add value to your organization:

- ❖ Strong privacy protections reduce risks associated with handling athlete personal information, leading to enhanced athlete trust in anti-doping processes and your organization;
- ❖ Building privacy into everyday anti-doping processes reduces compliance and legal and reputational risk;
- ❖ A privacy program will help you understand your data and operations, unlocking opportunities for new efficiencies and improving information governance;
- ❖ Implementing accountability in your privacy program will help you meet broader ethical and accountability expectations across the organization and make you a more trusted partner when receiving information from other ADOs.

2. Creating a privacy role, team or department

Recognizing the importance of making privacy protection a priority, the ISPPPI requires that ADOs designate a person to be accountable for the ADO's compliance with the ISPPPI. For the purpose of these Guidelines, we will call the designated person the Privacy Manager. You are free to choose a title of your choice, the important thing being that this individual will be focused on privacy matters.

WHO CAN BE A PRIVACY MANAGER?

Anyone can be a Privacy Manager. Ideally, appoint individuals that have some knowledge of data protection laws and requirements, that can advocate for privacy within the organization and are able to monitor how your organization processes personal information. Knowledge of information security or IT, as well as anti-doping, would also be helpful in performing this role.

If existing employees transferred to a privacy role or new hires do not already have this expertise, consider investing in their professional development. Also consider whether external consultants or professionals could fill this role or be hired to support an internal Privacy Manager. Under the ISPPPI, the Privacy Manager does not need to be exclusively dedicated to privacy. For large ADOs, consider supporting the Privacy Manager with additional team members. For smaller ADOs, you can also consider pooling resources by sharing a Privacy Manager with other ADOs.



In some jurisdictions, there may be independence requirements associated with the Privacy Manager role (or its equivalent) that prevent the individual from conducting other functions within the organization. There may also be additional requirements to consider for the role (e.g. a need to use a particular title, like Data Protection Officer, ability to report directly to upper management; protections from consequences for conducting functions, etc.).

WHAT IS A PRIVACY MANAGER RESPONSIBLE FOR?

The Privacy Manager should:

- ❖ Ensure that the ADO complies with the ISPPPI and applicable data protection and privacy laws;
- ❖ Ensure that the ADO has valid legal grounds to process personal information for anti-doping purposes (see [3. Applying ISPPPI requirements](#) in [Chapter 4: How to identify what you hold and why](#));
- ❖ Prepare, implement and regularly review the organization's internal privacy policies and procedures;
- ❖ Prepare records of processing (see [1. Creating a record of processing](#) in [Chapter 4: How to identify what you hold and why](#));
- ❖ Serve as the main contact within and outside the ADO for privacy-related inquiries, requests, or complaints (see [Chapter 10: How to respond to requests and complaints](#));
- ❖ Ensure that the retention times for personal information set out in Annex A of the ISPPPI are adhered to (see [Chapter 9: What personal information should be retained](#));
- ❖ If necessary, provide notice of a security breach to the relevant individuals (See [Chapter 7: How to prepare for and respond to a breach](#)); and
- ❖ Work with IT professionals to ensure appropriate safeguards for personal information are implemented (see [Chapter 6: How to protect personal information](#)).

Note that the ADO, not the Privacy Manager, is ultimately responsible for the ADO's compliance with the Code and the International Standards.

The Privacy Manager will need adequate resources to fulfill his or her role. Consider creating an annual budget for privacy or tasking your Privacy Manager with the preparation of this budget. A privacy budget may need to account for the following:

- ❖ Human resources (employee salaries, training costs, other expenses);
- ❖ Costs for external legal advisors, auditors, or consultants;
- ❖ Costs for privacy compliance software or other tools (e.g., e-learning vendors, or tools to create records of processing or manage privacy risks – see [1. Training your privacy champions](#) in [Chapter 11: How to create a privacy culture](#));
- ❖ Translation costs if you used WADA or other ADOs' resources that need to be translated into your own language. Make sure to use professional translators and have your Privacy Manager verify the accuracy of translations, ensuring that Code and IS language and the integrity of the work is intact;
- ❖ Costs for staff training materials and tools (see [2. Training your staff & raising awareness](#) in [Chapter 11: How to create a privacy culture](#)).

Where resources are limited, consider the minimum budget needed to implement your privacy program leveraging resources from other agencies, such as WADA's free ISPPPI templates, guidance, and courses available on ADEL.

HOW TO MAKE THE PRIVACY MANAGER ACCESSIBLE TO STAKEHOLDERS

Everyone in your organization should have access to the Privacy Manager and be encouraged to raise privacy questions and issues with this person.

The ISPPPI requires that the Privacy Manager’s contact information be readily accessible externally.

In practice, contact information for the Privacy Manager can be provided at the same time as other required information regarding the processing of personal information (see [Chapter 5: How to explain your processing practices](#)).

You are not obliged to provide the name of your Privacy Manager externally, but you can do so if you think this would be helpful. The important thing is to provide contact information where he or she can be easily reached (e.g. an email address, physical address, and/or phone number). It may also be helpful, especially for a general mailing address or phone, to specify the title or department to which correspondence should be directed (Privacy Manager, data protection officer, legal department, etc.).

The Foundations of Your Privacy Program

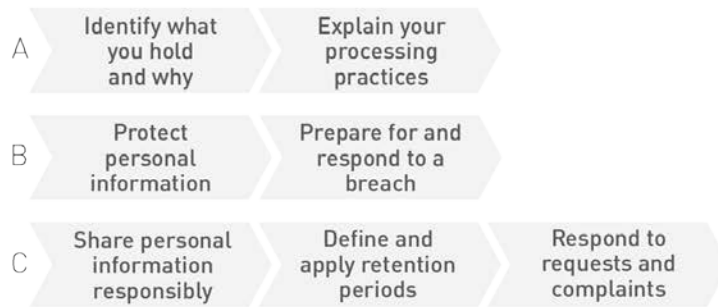
BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3



1. Understanding fair information principles

The ISPPPI is explicitly based on the Organization for Economic Cooperation and Development’s (OECD) 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines²).

The OECD Guidelines established eight principles for fair information management that laid the foundations of data protection legal frameworks around the world and, similarly, provide the foundations for the ISPPPI.

²<https://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflows ofpersonaldata.htm> (last accessed 14 October 2020)



Figure 1: Fair Information Principles in the ISPPPI³

³ The definitions and names of the eight fair information principles are not always verbatim. They have been adapted from the OECD Guidelines and summarized for simplicity and to use more up-to-date terminology.

2. Understanding the ISPPPI's place in your privacy program

The ISPPPI is mapped to the fair information principles, as shown in the image above. The purpose of the ISPPPI is to ensure ADOs take steps to implement each of these principles in their anti-doping activities.

Today's ISPPPI, combined with the Code compliance monitoring program, specifically focusses on ensuring that all ADOs achieve accountability with respect to their handling of personal information for anti-doping purposes. This aligns with the increased importance placed on this principle in privacy and data protection laws around the world, as well as the fair information principles themselves. In fact, the updated version of the OECD Guidelines contains a new section describing what is needed to implement the accountability principle:

"A data controller should:

- 1) Have in place a privacy management programme that:
 - i) gives effect to these Guidelines for all personal data under its control;
 - ii) is tailored to the structure, scale, volume and sensitivity of its operations;
 - iii) provides for appropriate safeguards based on privacy risk assessment;
 - iv) is integrated into its governance structure and establishes internal oversight mechanisms;
 - v) includes plans for responding to inquiries and incidents;
 - vi) is updated in light of ongoing monitoring and periodic assessment;
- 2) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
- 3) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects."⁴

The ISPPPI must also be understood in the context of the Code and other ISs. These documents contain a series of requirements that inform and lend context to the privacy principles set out in the ISPPPI.

⁴ OECD, Revised Guidelines on the Protection of Privacy and Transborder Flows of Information (2013), page 16, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last accessed 14 October 2020).

For example, what personal information is necessary to an ADO will be determined by what the Code and ISs require the ADO to collect for various anti-doping activities.

These Guidelines aim to provide ADOs with an understanding of how to implement the principles of the ISPPPI, as well as options and tools to achieve this objective.

3. Integrating privacy and data protection laws

The ISPPPI makes several express references to the need for ADOs to consider applicable privacy and data protection laws as part of their implementation of the ISPPPI.

As mentioned above, this is because, for most ADOs, there will be privacy and data protection laws that overlap with the ISPPPI. Given that the ISPPPI is based on the same principles as privacy and data protection laws around the world, you will likely find many similarities between it and laws applicable to your organization. ADOs should always consider the applicable privacy and data protection laws when building their privacy program.

ADOs should also consider and look to local laws governing sport and anti-doping. In some cases, these sport and/or anti-doping laws will specifically regulate the processing of personal information associated with anti-doping activities.

HOW TO KNOW WHAT LAWS APPLY TO YOU?

First, consider the location(s) from which you conduct most of your activities (e.g. your headquarters or main office). In most cases, this will determine the laws that apply to you.

Next, consider whether this location(s) has a data protection authority or regulator. If so, the website for this regulator is a great place to start to find guidance and information about local laws and their application.

Similarly, if there is a local sport or anti-doping law or policy in this location, consult the website for the government body responsible for this law or policy.

National Anti-Doping Organizations (NADOs) and International Federations (IFs) operating in the



Some laws use other criteria that seek to extend their application to activities that occur outside of the place where the law was enacted, like whether processing relates to individuals in that place or to the offer of goods or services to individuals in that place. In anti-doping, each ADO you collaborate with will be subject to its own laws, which could also impact you (e.g., if you provide anti-doping services to another ADO). This can make the task of identifying laws applicable to you complex.

In practice, focus on establishing a robust privacy program that complies with the ISPPPI and the laws where you are located. Where possible, follow the best practices described in these Guidelines and in those published by your local regulators. If you have the resources, you can seek legal advice to better understand your legal framework.

same location could explore opportunities for collaboration and information/expertise exchange in this regard.

Free tools, like the United Nations Conference for Trade and Development's tracker of Data Protection and Privacy Legislation Worldwide⁵, can also help you identify relevant privacy and data protection laws.

Law firms, other professional consultancy firms and industry trade associations⁶ may also offer free summaries, webinars, and other resources in their area of expertise, whether that is privacy, sport, or even information security. Look for local firms or local branches of international firms for information that will be most relevant to you.



⁵ See note 1.



⁶ See for instance, the International Association of Privacy Professionals (<https://iapp.org/>).

WHAT TO DO IF YOU THINK YOUR LAWS CONFLICT WITH THE ISPPPI?

The ISPPPI is a mandatory document, like the other ISs. It provides a floor, not a ceiling, of standards for the protection of personal information. This means that where an ADO is subject to applicable laws that set standards lower than the ISPPPI, the ADO must respect the higher standards of the ISPPPI. Where an ADO is subject to applicable laws that set standards that are higher than the ISPPPI, it must supplement the ISPPPI standards with the additional requirements under applicable laws.

The ISPPPI does contain a limited exception. In the event complying with the ISPPPI would place an ADO in conflict with other applicable laws, the ADO will not be deemed non-compliant with the Standard to the strict extent of the conflict. You should note that this would only occur in exceptional circumstances because applicable law will only very rarely preclude you from protecting personal information with the basic protections provided for in the Standard.

The following two scenarios illustrate the scope of the exception:

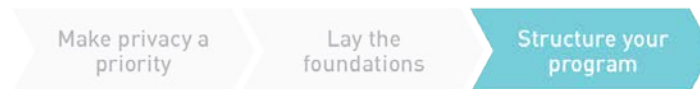
<div style="text-align: center;"> NO CONFLICT</div> <p>The ISPPPI requires that third-party agents be subject to appropriate contractual and technical controls when processing personal information to conduct anti-doping activities delegated to them by an ADO. The EU General Data Protection Regulation (GDPR) would require any 'processor' hired by an ADO to be subject to a specific set of mandatory controls. There is no conflict here because the ADO can comply with both the ISPPPI and applicable law.</p> <p>Similarly, an ADO that is not subject to any requirements to implement specific controls in an agreement with a third-party agent under applicable laws would be required to respect the ISPPPI requirement to do so. There is no conflict in this scenario either, because there is nothing that prohibits the ADO from complying with the ISPPPI requirement.</p>	<div style="text-align: center;"> CONFLICT</div> <p>An ADO is required to keep certain anti-doping data for 20 years due its relevance to certain penal or criminal doping offences under applicable law that can be prosecuted up to 20 years after their occurrence. The ISPPPI prescribes a maximum retention period of 10 years for the same data.</p> <p>In this scenario, there is a conflict because the ADO will be breaching the maximum retention period under the ISPPPI to comply with local law.</p>
--	---

In the event of a true conflict between the ISPPPI and applicable laws, you should communicate with WADA's compliance department at compliance@wada-ama.org as soon as reasonably possible and provide WADA with evidence of the specific conflicting requirement (e.g. the specific legal provision imposing the 20-year retention period). On this basis, the ADO would not be deemed non-compliant with the maximum ISPPPI retention period in the specific instances where a longer retention period is prescribed by a law applicable to the ADO. Where possible, the ADO should also inform other relevant ADOs of the conflict.

How to structure your privacy program

BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3



1. Identifying your governance structure

In Chapter 1, we reviewed the requirement to appoint a Privacy Manager, the responsibilities of the Privacy Manager, and human and financial resources to support the Privacy Manager.

In this chapter, we go beyond this basic requirement to help you structure your privacy program as a whole. First, the Privacy Manager should be supported by senior management within the ADO. This would typically be the people responsible for appointing the Privacy Manager and approving the privacy budget. Decisions around privacy may also require the input of other individuals or departments, depending on the complexity and structure of your organization.

To help you identify the governance structure at your organization, consider the following questions:

- ❖ Who is the ultimate decision-making person or body for the organization?
- ❖ Who reports to this person/body?
- ❖ Can you draw a reporting line from this person/body down to the Privacy Manager? If not, consider establishing one.
- ❖ Who approves budgets for the organization?
- ❖ On what basis are budgetary decisions made? Who is responsible for creating budget plans?
- ❖ Who else is involved in making key decisions for the organization? Legal? Operational leads? Financial officers? Consider how the Privacy Manager interacts with these functions.
- ❖ Do you already have governance committees or committees focused on risk, security, and/or information management? Consider formally including privacy matters within the terms of reference or formal responsibilities of these committees.

2. Assigning roles and responsibilities

Now that you have identified the existing governance structure at your organization, consider formally assigning roles and responsibilities for privacy from the top of the organization down to the Privacy Manager.

For instance, identify the decision-making person or body of the organization that is ultimately accountable for privacy, and outline how responsibility for privacy matters are delegated within the organization to the Privacy Manager (and others, if applicable).

Establish how the Privacy Manager is expected to report up to this decision-making person or body.

For larger organizations that have established a committee or group to discuss privacy matters, consider how often this committee should meet, who sets the agenda for the committee, and what issues should be discussed at this committee.

Identify roles that are complimentary to or closely linked to the privacy function, such as information security, information technology, risk and/or legal functions. Consider formally requiring these roles to support and complement each other.

3. Defining requirements that the organization must meet

In Chapter 2, we went through the privacy and data protection principles, minimum ISPPPI standards, and legal requirements that should form the basis of your privacy program.

Now that you have identified the framework, it is time to define specific requirements you will apply within your organization to meet the objectives of this framework. **These will be the 'internal policies and procedures' required by the ISPPPI.**

You can break it down by privacy principle, ISPPPI section, or operational area. For example, you can set up a privacy policy with each of the fair information principles acting as a section, under which you then

define concrete commitments and actions that your organization must take to comply with the principle. You could also use the ISPPPI articles to organize your document.

If you need help, look to the [ISPPPI Checklist](#) and the [ISPPPI in Practice Webinar](#) available on ADEL. [Section 2](#) of these Guidelines will also take you through implementation guidance for the key areas of your privacy program.

Consider questions like:

- ❖ What steps must we take to respond to a data subject request?
- ❖ How do we verify the privacy and information security practices of third parties we work with?
- ❖ What do we do to maintain security safeguards for the personal information we process?
- ❖ How do we explain to athletes and others how we will process their personal information?

It is important that your internal policies and procedures reflect the actual practices of your organization (or practices that you are confident can be implemented within your organization).

4. Writing it down and making it mandatory

Write down the requirements you have identified in internal policies and procedures to comply with the ISPPPI's documentation requirements. You should also consider documenting the governance framework you have built to support your Privacy Manager and privacy program.

You can create and format these documents in a way that best suits your organization and its existing policies and procedures in other areas. Typically, policies are used to set out higher-level requirements, such as the obligation to only process the personal information needed for a particular activity. Procedures can be added if you need to define a detailed process that must be respected, such as a procedure to assess new activities to ensure only necessary personal information will be processed. These requirements could also be integrated into existing employee codes of conduct or handbooks and the like.

In terms of making these requirements mandatory within your organization, **the ISPPPI requires that staff be subject to enforceable confidentiality obligations.** An enforceable obligation is one that can lead to disciplinary sanctions or other consequences if violated by an individual.

To help make sure accountability for privacy flows from the top of the organization throughout the whole organization, it is good practice to go beyond this ISPPPI requirement and formally require staff to review and acknowledge your internal privacy policies and procedures, possibly annually (see [Chapter 11: How to create a privacy culture](#)). Similarly, the violation of your internal policies and procedures should be subject to appropriate disciplinary sanctions.

SECTION 2:

Implementing your privacy program

Section 2 includes Chapters 4 to 10. This section will provide support for Articles 5.0 to 11.0 of the ISPPPI by helping you understand the personal information you hold and explain to others what you do with it (Part A); protect the personal information you process and prepare for a possible breach (Part B); and operationalize privacy in day-to-day actions like sharing personal information, deleting personal information you no longer need, and responding to requests and complaints (Part C).



Part A includes Chapters 4 and 5 and will provide support for ISPPPI Article 5.0 – *Processing Relevant and Proportionate Personal Information*; Article 6.0 – *Processing Personal Information in Accordance with a Valid Legal Ground*; and Article 7.0 – *Ensuring Appropriate Information is Furnished to Participants and Other Persons*. It will guide you through a process to identify the personal information you hold and explain what you do with it to others.

How to identify what you hold and why

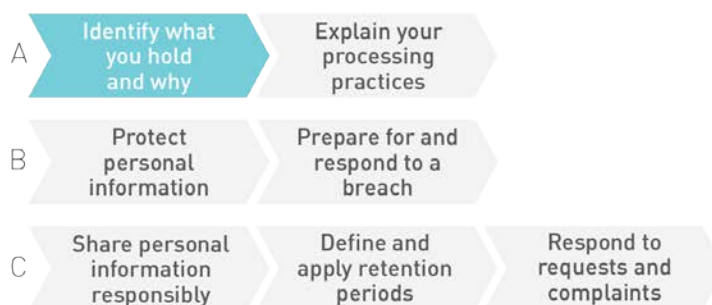
BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3



1. Creating a record of processing

ADOs must create and maintain what is called a ‘record of the processing’ for each of their activities that involve personal information. This is sometimes also called a ‘data inventory’ or a ‘data map’. This

record documents the personal information processed for a specific activity for which an organization is responsible.

The purpose of having these records, or data map, is to enhance an organization's accountability and ensure it has a proper grasp of the personal information that it processes. Otherwise, it can be difficult to adhere to the relevant privacy standards and requirements. Many privacy compliance activities are facilitated when you have a record of your processing activities. For example:

- ❖ You can use your record of processing to draft a privacy notice describing that processing;
- ❖ If you need to carry out a risk assessment of your processing, the work of understanding your processing will already have been done;
- ❖ If you experience a security breach, you can quickly identify impacted IT systems and data;
- ❖ If you are subject to complex legal requirements around data transfers or legal grounds for processing, having a detailed view of your activities will help you apply those requirements.

Before you get started, choose the format or tool that you will use to create and maintain these records. You could use a simple word document or an excel spreadsheet like the [Record of Processing](#) template. You could also use compliance software that is commercially available and that will have ready-made templates or systems for you to populate. Given that the creation of 'records of processing' became a mandatory requirement under the GDPR in 2018, many EU data protection authorities have also created template excel spreadsheets and guides to help you complete these records.

Once a format is chosen, make sure it will capture all of the information you are required to capture about your personal information processing. **Under the ISPPPI, the minimum information that you must include in the record for each processing activity is:**

- ❖ Why you are conducting it (i.e. the purposes of the processing);
- ❖ A description of the types of personal information involved;
- ❖ How long the personal information will be kept (or what criteria the storage period is based on);
- ❖ Who will have access to or receive this personal information (i.e. the categories of potential recipients);
- ❖ The measures taken to protect personal information when those recipients are other ADOs, third-party agents, or third parties; and
- ❖ How the personal information is protected more generally (i.e. a description of the technical and organizational security measures).



In some jurisdictions, ADOs may be required to keep a "record of processing" or similar document by law. This is case for ADOs subject to the GDPR. If this applies to you, make sure your record of processing contains any additional information you are required to include by law.

The ISPPPI does not set other requirements in terms of the format of the record or the types of information it must contain. For an example of a less conventional record of processing that still contains all of the information described above, take a look at the [ADAMS Privacy and Security FAQs](#), under the header, '[How information is collected, used and shared in ADAMS](#)'. This FAQ section, together with the description of security measures in ADAMS (under the header '[How is personal information protected in ADAMS](#)') responds to the ISPPPI requirement for WADA to maintain a record of processing that reflects the types of processing activities that occur in ADAMS. This record is intended to be a user-friendly, accessible

document that can be readily understood by athletes, other ADOs, or anyone who wants to understand how ADAMS works. Because anti-doping activities are standardized around the world, you can also use this webpage to help create your own records, keeping in mind that your records also need to reflect the elements of your processing activities that occur outside of ADAMS.

2. Identifying the facts

Now that you have the basic frame of your record of processing, you must populate it with relevant information. Throughout this process, your best guide will be someone that is responsible for each activity you wish to document. For instance, if you want to learn about any processing of personal information that occurs in connection with your education program, speak to your education manager. It may be helpful to involve personnel responsible for any associated IT system or database as well.

WHAT ACTIVITIES INVOLVE PERSONAL INFORMATION?

First, identify what activities involve personal information. If you are a larger organization, start at a department level and break down each department's day-to-day tasks. If you are a smaller organization, think about what each person does on a day-to-day basis.

For example, taking the person or department that is responsible for Therapeutic Use Exemption (TUE) management, they are likely responsible for some or all of these tasks:

- ❖ Create and improve the organization's processes for TUE management;
- ❖ Receive and review TUE applications;
- ❖ Receive and review requests to recognize a TUE;
- ❖ Respond to athlete questions about the TUE process;
- ❖ Respond to questions from other ADOs about a granted/denied TUE;
- ❖ Input TUE data into ADAMS;
- ❖ Track the amount and types of TUE applications received in a given time period; and
- ❖ Liaise with the organization's TUE Committee (TUEC).

Now that you have a comprehensive list of tasks, consider which ones can be grouped together as different steps of the same overarching activity. For instance, inputting TUE data into ADAMS is one step of the process of reviewing a TUE application. Also consider which tasks do not involve personal information – we have highlighted tasks in blue that may require further investigation to determine whether they involve personal information.

You may choose to group the above tasks into one record of processing for 'TUE management'. You may conversely want to break TUE management into a few different records of processing. This is ultimately at your discretion and will depend on how complex the different tasks are. Keep in mind that it can be time consuming to create and maintain these records, so you do not want to be so detailed as to make them unsustainable to maintain over time.

HOW IS PERSONAL INFORMATION COLLECTED, USED AND SHARED FOR EACH ACTIVITY?

For each activity you have identified at the previous step, you will need to document what types of personal information is collected, how it is used, and who it is shared with.

To do so, in keeping with our TUE example, consider the following questions:

- ❖ What personal information are individuals required to supply to apply for a TUE?
- ❖ How is this information collected, and who or what is it collected from?
- ❖ What is this personal information used for? Does any collected personal information go unused?
- ❖ Who is the personal information shared with?
- ❖ How is it shared?
- ❖ Where and how is the personal information stored?
- ❖ When and how is personal information deleted once it is no longer needed?
- ❖ Throughout the process, what systems or tools are used to collect, use, and share the personal information?

Note your responses in your record. It is always best to start with more detail and information and then refine your document on a second review.

HOW IS IT PROTECTED?

For ISPPPI purposes, you need to focus on two different types of protections for personal information:

- ❖ General protections; and
- ❖ Specific protections applied at the time of sharing personal information as part of a processing activity.

For general protections, consider the protections you have in place due to your overarching information security program (see [Chapter 6: How to protect personal information](#) or guidance). For instance, in the TUE example:

- ❖ Access controls: Only TUE managers have access to TUE applications in the physical filing cabinet we use and/or in ADAMS;
- ❖ Physical controls: The physical filing cabinet is locked; our office is only accessible with a key card;
- ❖ Technical controls: The computers we use to process TUE applications are protected by a firewall;
- ❖ Organizational controls: TUE managers have signed written confidentiality obligations.

To facilitate your work, you can always reference a description of your information security program and the security measures that are applied as part of this program to meet the requirement related to describing the technical and organizational measures that are in place.

For protections applied at the time of sharing personal information, investigate each type of sharing involved in your activity, and the types of protections applied for each one. For instance, in the TUE example:

- ❖ Sharing via ADAMS: A number of security measures in ADAMS exist that will apply to this sharing (e.g. encryption at rest and in transit, access controls, traceability of actions).
- ❖ Sharing with your TUEC: e.g., an encrypted communication channel, ensuring the TUEC members are subject to an obligation of confidentiality as required by the ISTUE, removing identifiers where not needed for the TUEC to examine an application.

3. Applying ISPPPI requirements

The next step after documenting the facts of your processing activity is to consider if your processing activity meets certain requirements. Ask yourself the following questions:

- ❖ Are you only processing what you need?
- ❖ Is the information accurate? Do you take any steps to ensure it is?
- ❖ What is your legal ground for processing?
- ❖ Are the individuals concerned properly informed of the processing activity?
- ❖ Do the individuals concerned understand the processing activity?
- ❖ Are you processing personal information for any purposes that are not anti-doping activities?

ARE YOU ONLY PROCESSING WHAT YOU NEED?

The ISPPPI requires that ADOs only process personal information necessary to their anti-doping activities. This requirement applies the principle of data minimization to anti-doping activities. It is also expressed in the ISPPPI as only processing personal information where relevant and proportionate for anti-doping purposes.

For ADOs, the first step to assessing if you are only processing what you need is to compare your processing of personal information to the requirements of the Code and ISs. In many cases, you will be required, under these documents, to collect specific personal information (e.g. the whereabouts filing requirements for athletes in a Registered Testing Pool (RTP) under the International Standard for Testing and Investigations (ISTI)).

If you find you are collecting more personal information than what is expressly required under the Code, consider whether you are adhering to the data minimization principle by only collecting relevant and proportionate personal information for your activities. For instance, for your second tier of athletes subject to whereabouts requirements, have you ensured that you only collect what you need to carry out no advance notice testing provided for in your testing plan for this athlete group?

IS THE PERSONAL INFORMATION ACCURATE?

The ISPPPI also requires that personal information processed by ADOs be accurate, complete, and kept up to date.

In practice, ADOs generally collect information directly from athletes, and should inform athletes of their obligation to ensure such information is accurate, complete, and up to date. Where possible, you should provide athletes with readily accessible means to access their own personal information and make required updates. For example, certain information contained within ADAMS can be updated directly by athletes at any time if you provide them with an account. You should also consider if there are steps you can take to verify and improve the accuracy of personal information held in various systems. For instance, consider if you are able to identify duplicate profiles in your databases.

WHAT IS YOUR LEGAL GROUND FOR PROCESSING?

Your legal ground for processing personal information will be dictated by the privacy and data protection laws, as well as sports and anti-doping laws, applicable to you ([3. Integrating privacy and data protection laws](#) in [Chapter 2: The Foundations of Your Privacy Program](#)). The requirement to have a legal ground for processing personal information is tied to the principle of lawful and fair processing. Processing of personal information will be lawful if it occurs in accordance with legal requirements, and it will be fair if it respects the expectations of the individuals concerned.

Historically, privacy and data protection laws often required organizations to obtain consent from individuals in order to process their personal information. In order to provide valid and meaningful consent, individuals needed to have knowledge of the relevant processing, hence the need for organizations to be transparent about their processing with individuals.

Today, the concepts of ‘knowledge and consent’ have been split in many legal frameworks. Transparency and the need to have knowledge of an organization’s processing of personal information has become its own distinct requirement.

Consent, for its part, continues to feature as a possible legal ground, however, many modern privacy and data protection laws provide for alternative legal grounds, for example:

- ❖ Compliance with legal obligations;
- ❖ Performance of public interest tasks;
- ❖ Processing necessary for public health purposes;
- ❖ Fulfillment of a contract;
- ❖ Processing needed for the legitimate purposes of an organization; or
- ❖ Dealing with legal claims or processes.



Under the UNESCO International Convention Against Doping in Sport, State Parties undertook to put in place appropriate measures to achieve the objectives of the Convention, including legislation, regulation, policies or administrative practices. Likewise, under the Code, ADOs set out their expectations that governments would implement measures for cooperation and sharing of information among ADOs and WADA. As a result, several countries have adapted their sport and anti-doping legislation to provide the legal grounds for processing personal information for anti-doping purposes.

Where alternative legal grounds to consent exist in a legal framework, these alternatives can be considered more appropriate for the anti-doping context by some. This is because anti-doping activities are a mandatory feature of sport and cannot be refused or rejected by athletes who wish to participate in sport.

Even if your jurisdiction generally considers consent to be a valid legal ground for anti-doping-related processing of personal information, there are often exceptions to consent that may apply to certain activities. For instance, in the context of an anti-doping investigation, you may be permitted to disclose personal information to law enforcement authorities, without consent, where there is a reason to believe that a violation of the law has occurred, or where compelled by an order from law enforcement.

Ultimately, you may need to consult legal counsel and your sport and data protection authorities to determine the legal grounds most appropriate to your anti-doping activities.

DO THE INDIVIDUALS CONCERNED UNDERSTAND THE PROCESSING ACTIVITY?

As mentioned in the previous section, regardless of the legal grounds you rely on to process personal information, you must make sure individuals understand and have knowledge of your processing. This is done by providing a privacy notice to individuals (see [Chapter 5: How to explain your processing practices](#)).

ARE YOU PROCESSING PERSONAL INFORMATION FOR ANY PURPOSES THAT ARE NOT ANTI-DOPING ACTIVITIES?

ADOs should only be processing personal information for anti-doping purposes in the context of 'anti-doping activities' provided for in the Code and ISs, as or required by law. These anti-doping activities include:

- ❖ Education;
- ❖ Testing and sample analysis;
- ❖ Managing the Athlete Biological Passport (ABP);
- ❖ Processing TUE applications;
- ❖ Gathering intelligence and conducting investigations;
- ❖ Results Management;
- ❖ Compliance monitoring and enforcement; and
- ❖ Anti-doping research

In the exceptional circumstances where you find that your organization is processing personal information for purposes not yet provided for in the Code or the ISs, **the ISPPPI requires that you carry out and document an assessment to ensure these purposes are relevant to the fight for clean sport.** This provision is intended to capture new or innovative anti-doping processes that may be developed in between Code review cycles. It will only be relevant in these limited circumstances.

To help you with this assessment, consider the following questions:

- ❖ How will this novel processing activity increase the effectiveness of the fight for clean sport? Is there any scientific or other evidence that demonstrates this is the case?
- ❖ Have stakeholders been consulted? Has WADA been consulted?
- ❖ What Code objectives does the processing activity seek to achieve?
- ❖ Even if this is a new activity, are there any relevant Code or IS provisions that are relevant to the activity?
- ❖ Are there any risks for individuals associated with this activity?

4. Assessing and mitigating risks

The final step, after documenting your processing activity and layering in ISPPPI requirements, is to assess and mitigate risks. If you have identified some gaps with respect to the ISPPPI requirements in the previous section, these should also be included in your assessment and mitigation of risks.

Under the ISPPPI, a risk assessment is only required for the processing of whereabouts information and sensitive personal information. This assessment must be repeated regularly. It is good practice to go beyond the ISPPPI requirement and carry out this assessment for all of your activities. If you critically assess your processing activities as you document them, you will find that you can easily and efficiently identify areas for improvement.

Although the ISPPPI does not define how often a regular assessment must occur, it would be prudent to assess at least on an annual basis. It would also be prudent to re-assess a processing activity when changes to this activity or to technical systems used as part of this activity are being considered.

Just as was done for your record of processing, start by creating a frame for recording your assessment and the measures you need to take to mitigate identified risks. See the [Risk Assessment Matrix](#) template for an example of how to identify and assess the risks of TUE management.

When carrying out your risk assessment, consider asking questions like:

- ❖ Are athletes (or other individuals) provided with **enough information** to understand how their personal information will be handled by Signatories, WADA, third party agents, and other third parties?
 - For guidance, see [Chapter 5: How to explain your processing practices.](#)
- ❖ Which staff have access to the personal information? Do they all need it to fulfill their duties? Can some staff fulfill their duties with more limited personal information?

- ❖ Is access to the personal information **limited and controlled** in each system where this information is stored or processed (e.g. internal documents, ADAMS, internal document management systems, etc.)?
- ❖ Consider if any **'privacy-by-design'** measures could be applied to each relevant system or application to mitigate the risks of the activity.
 - Privacy-by-design measures would include granular control over access privileges to ensure access on a need-to-know basis; automated data deletion processes; ensuring any such system or application only requires users to input relevant and proportionate information, etc.
- ❖ Is personal information **deleted** from each of these systems in accordance with ISPPPI Annex A?
- ❖ What **authentication requirements** (e.g. passwords, 2FA, etc.) exist for each of these systems?
- ❖ When personal information is shared, is it protected with **encryption, access controls**, or other measures?
- ❖ Have all recipients of personal information signed **confidentiality agreements**, or are they subject to statutory confidentiality obligations?



ADOs should consider whether specific requirements attach to such risk assessments, or whether additional assessments are required under applicable laws. For instance, an ADO may be required to complete a Data Protection Impact Assessment for its anti-doping activities, and regulatory authorities may have issued guidance setting out the information to be included in such an assessment.

If you are already carrying out more general risk assessments as part of a specific activity, consider building in privacy assessment questions to streamline your compliance with requirements under different ISs.

For example, ADOs have the discretion under the ISTI to collect different types and amounts of whereabouts information from different tiers of athletes. ADOs must conduct a risk assessment taking several factors into consideration when establishing these whereabouts tiers. Similarly, ADOs have the discretion to apply anti-doping rules to athletes other than international or national-level athletes, which will result in the collection of personal information in respect of such athletes. By building privacy into your existing assessment processes, you will have a more fulsome global assessment and you will be proactively mitigating risks.

How to explain your processing practices

BUILDING

SECTION 1

Make privacy a priority

Lay the foundations

Structure your program

IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3

Create a privacy culture

1. Preparing a privacy notice

ADOs must be open and transparent about their processing of personal information. This is achieved by providing notice to the relevant individuals that explains your data processing activities and related information before or when you collect the information from these individuals.

WHAT TO INCLUDE?

A notice should provide individuals with the answers to the following questions: Who, what, why, how, and what are my privacy rights and choices?

WHO?

ADOs must inform participants of:

- ❖ The identity of the ADO collecting the personal information;
- ❖ The contact details for their Privacy Manager; and
- ❖ The categories of organizations that will receive the personal information (for example, WADA, other signatories, or delegated third parties)

WHAT?

ADOs must describe the types of personal information that will be processed. Consult your record of processing to make sure your notice describes the types of personal information that will be processed for each relevant activity. For most anti-doping activities, this will typically involve basic contact and demographic information and information derived from sample analysis. Whereabouts information, medical information, and sanction-related information will also be processed for certain anti-doping activities.

WHY?

ADOs must explain why they process personal information, or in other words, what the purposes or objectives of their processing activities are. Be as specific as possible, considering the context in which individuals will see a particular notice. For instance, the mission of ADOs is generally to detect, deter and prevent doping in sport. However, the purposes that require the processing of personal information related to TUE management will be narrower, e.g. ensuring criteria for the granting of TUEs have been met.

HOW?

ADOs must explain how and in what ways personal information will be handled. At a minimum, this would include informing participants of:

- ❖ How long personal information will be retained, or the criteria used to determine this period;
- ❖ When and what personal information will be publicly disclosed in connection with an ADRV; and
- ❖ Other information necessary to ensure that the processing of personal information remains fair (see the information box below for more guidance).

WHAT ARE MY PRIVACY RIGHTS AND CHOICES?

Individuals must be informed of their privacy rights and choices under the ISPPPI (and applicable laws, if relevant) and how to exercise these rights and choices, as well as of the consequences of exercising these rights and choices. This would include informing participants of:

- ❖ Their right of access to personal information and the right to have information corrected, blocked or deleted if its processing is inaccurate, incomplete, or excessive;
- ❖ Their right to file a complaint with the ADO, the right to notify WADA if the complaint is not resolved, and where it exists, the right to submit a complaint to a competent data protection authority;
- ❖ The negative consequences that could arise from a refusal to participate in doping controls (such as a violation of the code, invalidation of competition results, or prohibition from participating in organized sport);
- ❖ That, even if they request the blocking or deletion of their information, or withdraw consent for its processing, ADOs may need to continue to process this information for investigations or proceedings relating to anti-doping rule violations, or to establish, exercise or defend against legal claims relating to the ADO, the individual, or both.



ADOs should also be aware of any special requirements under applicable law regarding their privacy notice. For instance, ADOs subject to the GDPR should review Articles 13 and 14 of the GDPR and determine if they need to provide additional information, such as: the legal basis or ground for their processing; details about any purely automated processing of personal information that might significantly affect individuals; information about transfers of personal information to another country (e.g. that such transfers entail certain risks, what legal mechanisms are used to effect the transfer and, potentially grant access to the mechanisms used – [Chapter 8: How to share personal information responsibly](#)); or information about any additional rights under applicable laws ([1. Understanding individual rights regarding personal information](#) in [Chapter 10: How to respond to requests and complaints](#)).

HOW TO DRAFT IT

Use clear and plain language when preparing your privacy notice, bearing in mind that individuals of different ages and reading comprehension levels will be receiving it. Think about the type of language used in your education programs – this is a good benchmark against which to review your privacy notices. Your privacy notices are intended to educate athletes about the ways in which you need to process their personal information for anti-doping purposes. There may also be tools built-in to word processing software that can

help you identify and adjust the reading level of your document. To make your privacy notices even more understandable, consider implementing other best practices like⁷ :

- ❖ Allowing individuals to control the amount of detail they wish to receive, and when;
- ❖ Considering the perspective, ages and reading comprehension levels of the individual when designing your notice;
- ❖ Adopting innovative and creative ways of providing notice, which are just-in-time, specific to the context, and suitable to the type of interface (e.g. making use of videos, infographics, icons, etc.);
- ❖ Involving user interaction/user experience (UI/UX) designers;
- ❖ Consulting with privacy experts and/or regulators; and/or
- ❖ Bringing material changes to your privacy notice to the attention of relevant individuals.

2. Providing your privacy notice to the right people, at the right time, in the right way

WHEN AND HOW TO PROVIDE A PRIVACY NOTICE

Your privacy notice must be provided to individuals before or at the time of collecting personal information from them (see [When can you delay providing this notice?](#) below for limited exceptions).

Examples of where you might provide a privacy notice before collecting personal information could be a general privacy notice you post on your website for information purposes, or a privacy notice you include as part of your anti-doping rules. Examples of privacy notices provided at the time of collecting personal information could be a privacy notice included in your Doping Control Form, in your license application form, in your event registration form, or as part of an athlete's login to your organization's anti-doping system.

We recommend that ADOs provide both:

- ❖ general privacy notices that are readily available; and
- ❖ specific notices at points of interaction with athletes that involve the collection of personal information.

It may be helpful for you to map out the athlete journey and identify contexts or events where you will have a direct interaction with athletes, for example, a licensing or accreditation application/registration, a sample collection session, a TUE application, the inclusion in a testing or education pool, etc. These are good opportunities for you to include a privacy notice in the information you provide to athletes. If third-party agents will be acting on your behalf in any of these scenarios, make sure they are equipped with your approved privacy notice, or that you have reviewed and approved the privacy notice they intend to use.

⁷ Adapted from the Guidelines for obtaining meaningful consent, Office of the Privacy Commissioner of Canada (May 2018), https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ (last accessed 14 October 2020).

Remember that ADOs can also be third-party agents when they are carrying out an anti-doping activity, like a sample collection session, under the authority of and as delegated by another ADO.

You can provide a privacy notice verbally, in writing, or via visual means like videos or icons. It is good practice in all cases to keep a record of the notice you provide. This will also be important to demonstrate your compliance as part of a WADA compliance audit. For example, if you provide verbal notice at a sporting event explaining that doping controls could be conducted and will involve the processing of personal information, you could keep a record of the information staff were trained to provide to individuals.

WHEN CAN YOU DELAY PROVIDING THIS NOTICE?

ADOs may delay providing a privacy notice to individuals where providing such notice might reasonably jeopardize an ongoing or anticipated anti-doping investigation or undermine the integrity of the anti-doping process.

This would only be permissible in limited circumstances, and, in many cases, ADOs should still be able to provide advance notice of the type of processing of personal information they carry out that may not be immediately obvious to an athlete or other individual.

In all cases, appropriate notice should be provided to individuals as soon as reasonably possible, and if there was a need to delay providing this notice, the justification for the delay should be documented.

The following two examples illustrate how ADOs can provide advance notice of their processing activities.



NO ADVANCE NOTICE TESTING EXAMPLE

A passport custodian IF has an arrangement with a partner NADO, whereby the partner NADO carries out a certain number of ABP tests upon request of the passport custodian acting on intelligence related to athlete biological passports. The NADO will be the testing authority and will include the tests as part of its own testing program.

The passport custodian IF would need to provide the NADO with the whereabouts needed to carry out a testing mission for athletes that are not nationals of the NADO. At the time of carrying out the sample collection, the NADO will need to provide a privacy notice to the athlete explaining how it will process the athlete's personal information. The NADO could not have sent a privacy notice to the athlete at the time of collecting the whereabouts information without undermining the integrity of the no advance notice test. The athlete should already have been informed, however – by the passport custodian and/or the athlete's principal NADO – of the possible receipt of his or her personal information by other anti-doping organizations having authority to test him or her, and the purposes for which passport and whereabouts information would be used.



INVESTIGATIONS EXAMPLE

If an ADO is investigating an individual who is not an athlete, and who therefore may not have received the ADO's privacy notices in the course of a doping control or in other anti-doping contexts, the ADO may not be able to inform the individual of the processing of his or her personal information until the investigation is complete. The ADO should, however, take measures to ensure that any person subject to its rules receives (or at a minimum, has access to) information about how it will process personal information, including in the context of an investigation. This example shows why having a general privacy notice that is readily available can be particularly useful for ADOs.

WHERE TO FIND HELP

There are many WADA templates you can use to help provide appropriate privacy notices at relevant moments in the athlete journey:

- ❖ WADA's Doping Control Form template contains a privacy notice you can use to provide notice as part of a sample collection session;
- ❖ WADA's TUE Application Form template contains a privacy notice tailored to the TUE context; and
- ❖ The Anti-Doping Privacy Notice template (long form) can be used as a general anti-doping privacy notice.
- ❖ The Anti-Doping Privacy Notice template (short form) can be used in other forms that athletes are required to complete or receive, such as a license application or event registration form.

3. Obtaining valid consent if you need it

As we saw above (see [What is your legal ground for processing](#) in [3. Applying ISPPPI requirements](#) of [Chapter 4: How to identify what you hold and why](#)), valid consent is closely linked to providing appropriate notice. The basic principle is that an appropriate notice is needed for the consent to be informed, and therefore, valid.

CONDITIONS FOR VALID CONSENT

More specifically, **under the ISPPPI, consent must be informed, freely given, specific and unambiguous**. Generally, if you have followed the requirements and best practices for privacy notices that we described in these Guidelines, you will be well positioned to demonstrate that you have met the conditions for valid consent. In this next section, we will focus on the additional steps to take if consent is your legal ground to process personal information.

For consent to be **informed and freely given**, individuals must have been provided with all of the ‘who, what, why, how, and what are privacy my rights and choices’ details described above (see [Chapter 5: How to explain your processing practices](#)). It is particularly important to describe the negative consequences that could result from refusing to provide consent to personal information processing, and to describe circumstances where you may need to keep processing personal information even after consent is withdrawn.

Tailoring your privacy notices to the specific context (for example, a sample collection session or a TUE application) is what will help you meet the requirement of a **specific and unambiguous** consent. You should also include a mechanism for the athlete to confirm their understanding of your privacy notice and affirmatively agree to your processing of personal information (for example a signature, a tick box, an ‘Accept’ or ‘Reject’ button). This becomes a requirement when dealing with sensitive personal information, for which you will need to obtain ‘explicit’ consent.

‘**Explicit**’ consent is a slightly higher bar than ‘specific and unambiguous’ consent. The difference between the two standards is not particularly great, however. All consent must involve a specific, informed and unambiguous indication of the individual’s wishes.

The key difference is that ‘explicit’ consent must be affirmed in a clear statement (whether oral or written), whereas an unambiguous consent can include a consent that can be inferred from an individual’s actions.

An example of an unambiguous, but not explicit consent, might be where an athlete is clearly told about the consequences of setting up an online account in an anti-doping database and proceeds with the set up. An explicit consent would be where an athlete is presented with an anti-doping form, and applies his or her signature or ticks a box to evidence consent to the collection and processing of their information.

WHAT ADAPTATIONS TO CONSIDER FOR MINORS AND PROTECTED PERSONS

Where an individual is incapable of providing a valid consent by virtue of their age (minors), mental capacity or other legitimate reasons recognized in law, a parent, legal guardian, or other representative can provide consent on the individual’s behalf. Consider including a space in your privacy notice or consent form to document the consent of a parent or other representative on behalf of an individual, where relevant.

Where possible, ADOs should verify the relationship between the individual and the representative. This verification does not necessarily require separate documentation. For example, a parent could accompany a minor athlete during a sample collection session at a sporting event, where the minor verbally confirms the relationship. Where the representative has a more remote relationship with the individual, it may be prudent to require documentation, for example, a coach or trainer could have been supplied with a letter signed by a parent authorizing them to sign a document for a minor athlete on the parent’s behalf.

HOW TO DEAL WITH A REFUSAL TO CONSENT OR A WITHDRAWAL OF CONSENT

Any refusal or withdrawal of consent will require a case by case assessment of the circumstances. At a high-level, refusing to consent to anti-doping rules that require the processing of personal information may render the individual ineligible to compete in further sporting events.

At a more granular level, depending on the timing, you may need to determine if the refusal or withdrawal amounts to an Anti-Doping Rule Violation (ADRV) under the Code (e.g. under Article 2.3 – Evasion, Refusal or Failure to Submit to Sample Collection, 2.4 – Whereabouts Failure, or 2.5 – Tampering).

You will also need to determine if you need to continue processing personal information to meet obligations under the Code (e.g. to conduct investigations or sample analysis or to complete results management procedures related to possible ADRVs) or to establish, exercise or defend yourself or others against legal claims.

In all cases, you should keep the individual informed, provide reasons for your actions, and follow the other processes described in [Chapter 10: How to respond to requests and complaints](#).

PART B: PROTECTING PERSONAL INFORMATION AND PREPARING FOR A POSSIBLE BREACH

Part B includes Chapters 6 and 7 and will provide support for Article 9.0 of the ISPPPI – *Maintaining the Security of personal information*. It will help you understand what you need to do to protect personal information, how to prepare yourself for a security breach, and what to do in the event of a security breach.

How to protect personal information

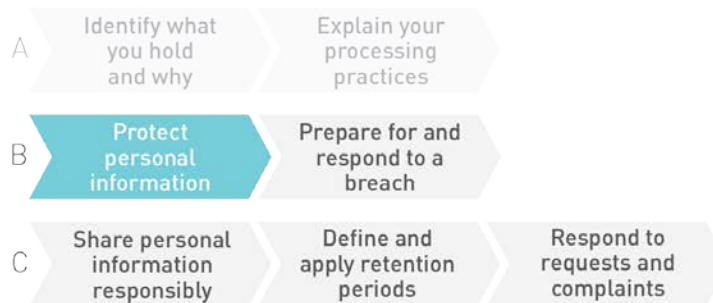
BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3



1. Building and implementing an information security program

ADOs have a responsibility to protect the personal information in their possession by applying security safeguards appropriate to the sensitivity of the personal information. This includes physical,

organizational, technical, environmental and other measures. The purpose of these safeguards is to protect personal information from a security breach.

The concept of a security breach is broad under the ISPPPI – it is a “breach of security resulting in the loss, theft, damage or unauthorized or unlawful processing of personal information (...), or interference with an information system, that compromises the privacy, security, confidentiality, availability or integrity of personal information”.

To effectively protect personal information, and comply with this ISPPPI requirement, ADOs need to build and implement an information security program. An information security program is a key component of your privacy program, but it is also its own distinct program that requires dedicated human and financial resources.

To better understand where privacy and information security overlap, consider the following graphic, that illustrates the different risks that privacy and information security programs seek to address:

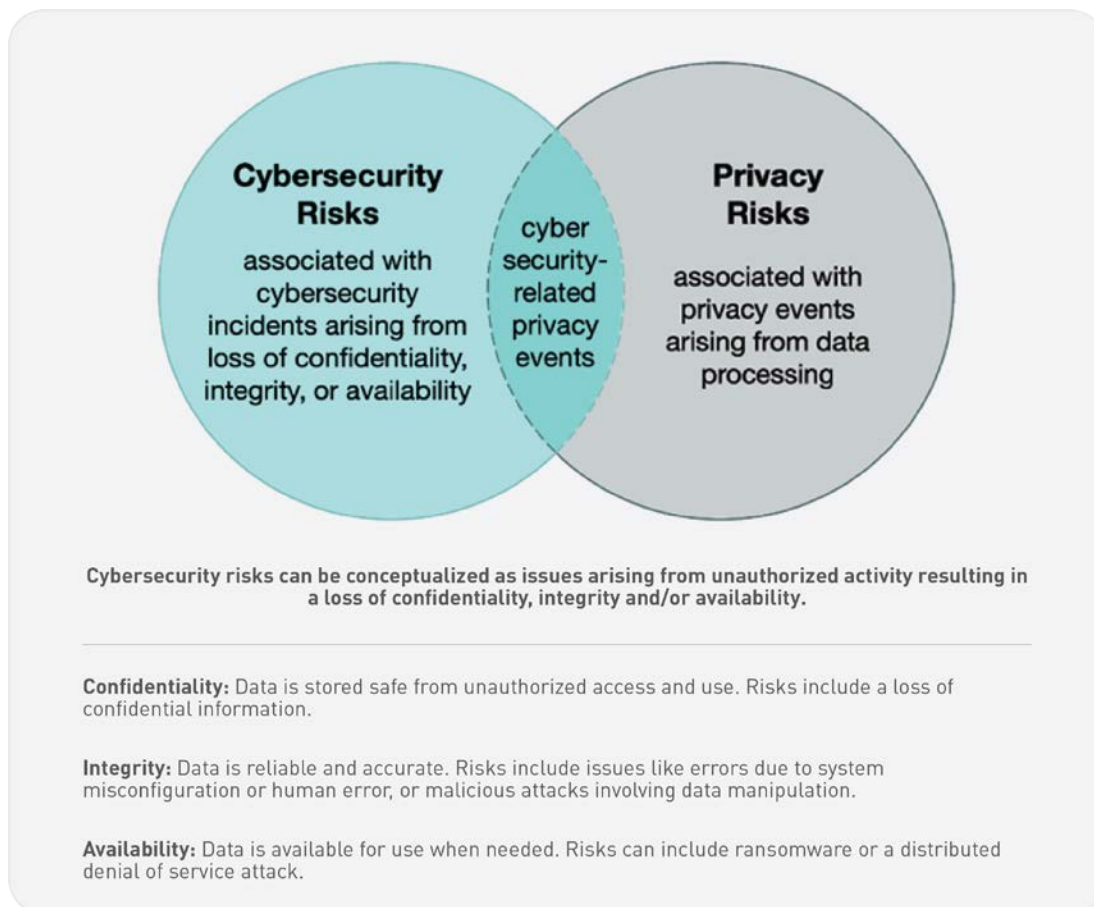


Figure 2 – Privacy and Cybersecurity Risks⁸

⁸ Adapted from the NIST (National Institute of Standards and Technology (US Dept of Commerce) Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0, January 16, 2020

Cybersecurity risks overlap with privacy risks when they impact personal information, for example, a loss of personal information or a ransomware attack involving a system that houses personal information. Conversely, if a distributed denial of service attack takes down your website, there is typically no overlap with privacy concerns.

It is important to remember that, while an information security program is critical to protecting personal information against certain types of risk, it will not suffice to address all privacy risks. For example, consider a system that has been programmed to collect certain data: the system is functioning correctly and securely, but it is in fact collecting too much data in violation of the data minimization principle. This privacy risk would only be identified upon assessing the data processing activity and related IT systems as discussed in [Chapter 4: How to identify what you hold and why](#).

WHAT ASSETS DO YOU NEED TO PROTECT?

Just like your privacy program, a good place to start when developing an information security program is understanding the information you hold, your business activities, and the systems, applications, and software used to process the information.

WHAT ARE THE RISKS?

Next, to understand the cyber risks you face, catalog the effects of any loss of confidentiality, integrity, or availability for each of your information assets. You should consider these effects from the dual perspective of your operations and the people whose information you hold.

WHO IS RESPONSIBLE FOR THEM?

Finally, you need to assign responsibility for protecting your assets. Consider whether you have the skills internally, whether you need to hire more staff, or whether you can outsource responsibility for certain parts of your program to external experts or service providers.

2. Implementing appropriate security safeguards

You will need a combination of different security safeguards to effectively protect personal information. In this next section, we will review practical examples of measures you can implement in the four categories referenced in the ISPPPI.

(Figure 2: Cybersecurity and Privacy Risk Relationship).
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf> (last accessed 14 October 2020).

We also encourage you to listen to the ISPPPI Webinar, Cyber Security Essentials for ADOs, for more guidance on implementing security safeguards. Many governments or regulatory authorities have also published cyber and data security guidance⁹.

WHAT ARE PHYSICAL AND ENVIRONMENTAL MEASURES?

Physical security measures include:

- ❖ Locked file cabinets;
- ❖ Card access systems;
- ❖ Physical keys;
- ❖ Sign-in logs for visitor access to physical offices, doping control stations, data centers, or other locations where personal information is processed or stored;
- ❖ Camera surveillance of entry/exit points; and
- ❖ Secure disposal of confidential physical files (e.g. shredding).

Environmental measures are measures to protect against accidental loss or destruction of personal information as a result of environmental factors or incidents, such as fire, flood or power failure. Examples include smoke detectors and fire suppression systems.

If you own or rent office space in an office building, it is possible the building owner or manager is responsible for implementing a number of these measures. Take stock of your specific office space and document the physical and environmental measures in place.

If you use cloud-based services, your cloud provider is typically responsible for implementing appropriate physical and environmental protection measures to protect its data centers. Review agreements you have with these providers or ask your account representative for details about the safeguards that have been implemented for the specific data centers where your data is located.

WHAT ARE ORGANIZATIONAL MEASURES?

Organizational measures include:

- ❖ Information security policies and procedures;

⁹ See for instance: Baseline Cyber Security Controls for Small and Medium Organizations (Government of Canada), <https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>; Data Security Guidance (Irish Data Protection Commission), <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance>; Cyber Essentials (National Security Centre, UK), <https://www.ncsc.gov.uk/cyberessentials/advice>; CNIL Guides, Security of Personal Data, 2018 edition, https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf; BSI IT-Basic Protection Compendium (Germany), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Kompendium/IT_Grundschatz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=7; Code for Cybersecurity Law (Spain), https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1 (for all of the foregoing, last accessed 14 October 2020).

- ❖ Background checks for new hires;
- ❖ Staff training and awareness (see [Chapter 11: How to create a privacy culture](#));
- ❖ Ensuring personnel are subject to confidentiality obligations; and
- ❖ Implementing approval processes to limit access to personal information on a need-to-know basis.

You may ask what ‘**need-to-know**’ means in practice. This is a term closely linked to the ‘data minimization’ principle, and it involves both organizational and technical controls. Consider the following example:



ACCESS CONTROL EXAMPLE

Jen is an Education Manager at an ADO. She is responsible for creating and implementing an Education Plan, and for monitoring completion of mandatory training courses by athletes in her ADO’s testing pools on ADEL. Jen requests an ADAMS account to download the most up to date list of athletes within the ADO’s testing pools and cross-reference this list against athletes having completed courses on ADEL.

The ADAMS Manager asks Jen a few questions to clarify her request:

Q: (ADAMS Manager) How often do you need to check the latest athlete list?

A: (Jen) Not very often. I usually do a cross-referencing every few months with my ADEL list.

Q: Do you need access to ADAMS for any other reason?

A: I don’t think so.

Q: Is the athlete list available in an excel sheet or another document outside of ADAMS?

A: I think so, or at least, I could probably ask someone with an account to download it for me.

Based on Jen’s responses, the ADAMS Manager refuses Jen’s request. She explains that it would be best for Jen to use the excel version of the athlete list that a colleague can download for her. This way, Jen will only access the relevant athlete list, rather than additional personal information that would have been available to her with an ADAMS account. She explains that this solution also makes more sense from a security perspective, because it is one less account that can be compromised through a phishing or other cyber attack.

An ADO's access control procedures should cover the granting of access permissions, the monitoring and updating of these permissions, and the removal of permissions when a person's role and responsibilities change. For example, if Jen moves on to a new role as testing manager, she will then probably need an ADAMS account to plan and monitor tests. However, she may no longer need an ADEL account.

WHAT ARE TECHNICAL MEASURES?

Technical security measures help bolster an organization's information security posture by protecting against human error and action.

Technical security measures include:

- ❖ Authentication requirements (e.g., unique logins, complex passwords, and second or multi factor authentication steps, such as TOTP or SMS codes, biometric authentication, etc.);
- ❖ Technical access restrictions (e.g. isolating or segmenting networks or databases);
- ❖ Encryption, including for any transmitted information;
- ❖ Logging and monitoring of user access and activities to ensure access restrictions are respected and to help detect any unauthorized access or suspicious activity;
- ❖ Anti-virus software and firewalls;
- ❖ Applying system upgrades and patches;
- ❖ Requiring a VPN for remote access;
- ❖ Using mobile device management software; and
- ❖ Applying automatic screen locks and logoffs on all devices.

How to prepare for and respond to a breach

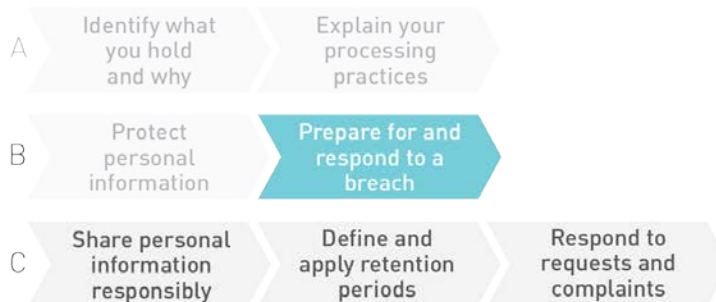
BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3



1. Creating a response plan

To help better prepare for a security breach, ADOs should implement a security breach preparedness and response plan and test it to ensure that it works.

WHO IS YOUR INCIDENT RESPONSE TEAM?

First, identify your response team. You will need a diverse set of skills to respond to a security breach, including legal, privacy, IT, communications, and management. Make sure your team includes leaders for each of these key response areas.

WHAT WILL THEY BE RESPONSIBLE FOR?

Next, document what each team member is responsible for. Consider naming a team leader or coordinator (e.g. the Privacy Manager) to ensure someone is ultimately responsible for managing the various aspects of your security breach response. Do not forget to assign responsibility for related activities, like training, reviewing and updating the plan on a regular basis, and creating record-keeping processes to log information about each security breach.

You should also ensure your staff are instructed on how to respond promptly to a security breach.

For example, your staff should be responsible for immediately notifying the response team of a suspected incident, for complying with instructions from the team to respond to the incident, and for retaining any relevant records in case those are helpful in dealing with the incident. They should also participate in any breach response training offered to them.

WILL YOU NEED HELP FROM THIRD PARTIES?

Consider whether you will need third party assistance as part of your response to a security breach. Would you need a forensic investigator to identify the source and cause of a breach? Would you need external legal support, or the help of a public relations firm?

Certain breach response providers (such as forensic investigators) offer retainer solutions with no upfront cost to the client organization. The advantage of this retainer is that the organization then has immediate access to the provider in the event of a breach, and it is not necessary to spend any time establishing the relationship.

You may also wish to review your insurance policies to determine if you have obligations to involve your insurer in the event of a breach.

Once you have identified external third parties that you would be in contact with in the event of a breach, make sure you document their functions or role and contact information in your plan.

HOW TO MAP OUT RESPONSE STEPS

Your response plan should address and assign responsibility for five key steps: discovery, containment, assessment, notification, and remediation. These steps may occur simultaneously depending on the type of breach and how it evolves.

ADOs should review applicable laws and layer in or adapt each of these response steps according to requirements applicable to them.

Discovery

Document who should be notified in the event of a security breach. **The ADO's Privacy Manager must feature among those that are first to be notified.** Identify any specific number or helpline to be used by staff for purposes of this notification.

Once an incident has been reported, the Privacy Manager (or other response coordinator) should document all available information regarding the breach. Consider the following questions:

- ❖ When was the breach discovered?
- ❖ What is the date or time period during which the incident occurred?
- ❖ What is the nature and cause of the incident?
- ❖ What types of individuals are affected, and how many?
- ❖ What systems are affected or involved in the breach?
- ❖ What types of personal information are affected?
- ❖ What possible harms could result from the breach?

Use the [Security Breach Reporting Form](#) template, or create your own, to gather and record the relevant details.

After an initial assessment of the breach, the Privacy Manager should update other relevant members of the response team to discuss and implement appropriate containment, notification, and remediation measures in accordance with the security breach response plan.

Containment

Document who is responsible for identifying and taking appropriate containment steps. This could involve:

- ❖ IT-based containment steps (such as taking systems offline; forcing password resets; or launching a forensic investigation);
- ❖ legal steps (such as invoking legal rights under contracts where the breach was caused by a third party), or
- ❖ other steps (such as communicating internally and externally to warn other relevant parties of the breach and minimize its impact).



Assessment

The Privacy Manager and response team must investigate and assess the breach to understand its nature, scope, impact, and severity. This is a key step to ensuring appropriate containment and notification requirements are met.

For instance, the loss by a staff member of a laptop containing limited, non-sensitive personal information that is encrypted and can be remotely wiped will give rise to a different set of containment, notification, and remediation steps than a ransomware attack by a malicious, motivated attacker affecting files containing a high volume of sensitive personal information.

You will also need to assess the security breach to determine whether you are required to inform the individuals concerned. This will be the case where the breach is likely to affect the individual's rights and interests in a significant way ([3. Responding to a breach](#) in [Chapter 7: How to prepare for and respond to a breach](#)).



Notification

Document your notification and reporting obligations. Consider circumstances where you may need to notify the following groups:

- ❖ Affected individuals;
- ❖ Regulatory authorities;
- ❖ Other governmental entities;
- ❖ Affected ADOs;
- ❖ Other affected third parties; and
- ❖ Where a breach involves or may involve illegal activity, law enforcement or other authorities.

WADA generally encourages ADOs to communicate and collaborate with WADA and other ADOs that may be affected by the breach or that have a relationship with the affected persons. Where a security breach affects ADAMS, ADOs are required to promptly notify WADA of the breach.

Beyond your notification obligations, it is a good idea to also document and assign responsibility for managing internal and external communications. Staff may need to be kept informed of steps they need to take to remediate or contain a breach, and, in the event of a major incident, you may need to respond to media or other public inquiries.



Security breach notification obligations are becoming increasingly common throughout the world, and ADOs may well be required to comply with obligations that go beyond the ISPPPI in respect of security breach notification obligations. ADOs may also be subject to contractual obligations to notify third parties in the event of a breach.



Remediation

Remediation measures following a security breach will vary depending on the cause, nature and circumstances of the breach. They may involve enhanced security safeguards, disciplinary sanctions for persons found to be the cause of the security breach, and increased training and awareness for personnel.

Ensure your plan includes requirements to assess and implement appropriate remediation measures following a breach. It may be helpful to conduct a post-incident debrief of the team to identify lessons learned and prevent a future recurrence. Do not forget to assign responsibility for monitoring the implementation of any identified remediation measures.

Note that you must also maintain appropriate records regarding the security breach, including the facts related to the breach, its effects, the ADO's assessment of the breach, and remedial actions taken. You can use the [Security Breach Log](#) template to document these details, or create your own.

2. Testing your plan

Now that you have created your plan, you should test it. How? Testing your plan can be as simple as using a real-world breach incident reported in the papers, and imagining it has occurred within your organization. Typically, the person running your test session would start by presenting the initial 'discovery' details of a breach to the response team. As you go through the response steps, the person running the session should provide the response team with new information to simulate the dynamic nature of breach response.

You can also seek out the assistance of a third party to help you run a test. Many information security consultants or firms will offer this service.

Conducting this type of test will help you achieve several objectives, including:

- ❖ Testing the effectiveness of your response processes in a safe, no-risk space;
- ❖ Solidifying your response team's understanding of the response plan, and of their responsibilities;
- ❖ Ironing out your communication channels (e.g. how will you keep the response team updated and aligned); and
- ❖ Gaining insight into your strengths and weakness when it comes to breach response.

After the test, debrief with your team to identify improvements you should make to your plan.

3. Responding to a breach

In the unfortunate event you suffer a security breach, you will need to activate your plan and respond. A key part of that response is assessing a security breach to determine which notification and other remediation steps must be taken.

HOW TO ASSESS A SECURITY BREACH

Under the ISPPPI, you must notify affected individuals of a breach where it is likely to affect their rights and interests in a significant way.

To determine if a breach meets this standard, you will need to assess the severity and impact of a breach. To guide your assessment, consider questions like:

- ❖ What types of personal information were breached and under what circumstances? Have multiple types of personal information been breached?
- ❖ How likely is it that someone would be harmed by the breach (e.g. by suffering emotional or psychological distress, discrimination, identity theft, damage to reputation, economic harm)?
- ❖ How long has the personal information been exposed?
- ❖ Is there evidence of malicious intent (e.g. theft, hacking)?
- ❖ Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm (e.g. in the case of an accidental disclosure to unintended recipients that commit to destroying and not disclosing the data)?
- ❖ Conversely, was the information exposed to individuals/entities who are unknown, to a large number of individuals, to entities/individuals who are likely to attempt to cause harm with it (e.g. hackers), or to individuals that represent a reputation risk to the individual?
- ❖ Has harm materialized (i.e. do you know data has already been misused)?
- ❖ Was the information lost, inappropriately accessed or stolen?
- ❖ Has the personal information been recovered?
- ❖ Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

Factors like adequate encryption or other safeguards, or the limited nature of the breach involving exposure to known entities that have deleted the relevant information, will tend to mitigate the severity and impact of a breach. Conversely, a high volume or high sensitivity of breached personal information, or the exposure of this information to individuals or entities with malicious intent, will increase this severity and impact.

WHEN AND HOW TO NOTIFY AFFECTED INDIVIDUALS

If you have determined that you must notify affected individuals about a breach, **the notice must be sent as soon as reasonably possible**. This means that after you discover a breach, you must act quickly to gather relevant details, assess the breach, and then prepare your notification to individuals.

The notification must include the following details at a minimum:

- ❖ The nature of the breach;
- ❖ The possible negative consequences for the persons concerned; and
- ❖ The remediation measures taken or to be taken by the ADO.



You may be subject to different timing obligations for notifications to be provided to individuals, regulatory authorities, or other organizations under applicable laws. For example, you may be obligated to provide such notice within 72 hours, where feasible, or without undue delay. Look to regulatory authority guidance on how to interpret and apply these timing requirements.

Notice can be provided by any appropriate means, including verbally or in writing, considering the circumstances of the breach as well as the prejudice that the relevant individuals may suffer as a result of the breach. Just as you would do for a privacy notice, use clear and plain language in your notification, and consider the perspective of the recipient of this information. Consider also creating a notification template in advance that you can then complete with the relevant details in the event of a breach.

WHEN AND HOW TO NOTIFY OTHER ORGANIZATIONS

As mentioned above, WADA encourages ADOs to communicate and collaborate with WADA and other ADOs that may be affected by the breach or that have a relationship with the affected individuals. Where a security breach affects personal information processed via ADAMS, ADOs are required to promptly notify WADA of the breach.

ADOs may be required to notify a regulatory authority for privacy or data protection. ADOs may also be strongly encouraged or required to notify cyber security centers or threat intelligence networks in the event of a malicious attack, or law enforcement in the event illegal activity is suspected.

Under the ISPPPI, there are no mandatory timing or content requirements for notification to other organizations.

WHAT OTHER REMEDIATION STEPS DO YOU NEED TO TAKE?

In addition to notifying affected individuals and organizations, there are many steps you can take to remediate a breach. The specific measures will depend on the nature of the breach you suffered. They could include:

- ❖ Re-training or providing more training to staff;
- ❖ Isolating or disabling compromised systems;
- ❖ Changing all passwords on compromised systems;
- ❖ Remote wiping lost or stolen devices;
- ❖ Monitoring logs, systems and networks for signs of suspicious activity; or
- ❖ Restoring lost information from a backup.

HOW TO IMPROVE YOUR FUTURE RESPONSE

As always, to improve how you manage any future breaches, build in time with the breach response team after dealing with a breach to take stock of the failures or gaps that led to the breach, the positive and the negative aspects of your response, and the lessons learned throughout the process. Document these lessons in your record/log of the breach or another document, and update your breach response plan as needed.

Part C includes Chapters 8, 9 and 10 and will provide support for ISPPPI Article 8.0 – *Disclosures of Personal Information to other Anti-Doping Organizations and Third Parties*; Article 10.0 and Annex A – *Retaining Personal Information Where Relevant and Ensuring its Destruction*; and Article 11.0 – *Rights of Participants and Other Persons with Respect to Personal Information*. It will help you manage risks associated with sharing personal information, ensure you do not keep personal information longer than you need it, and respond to requests and complaints about your privacy practices.

How to share personal information responsibly

BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



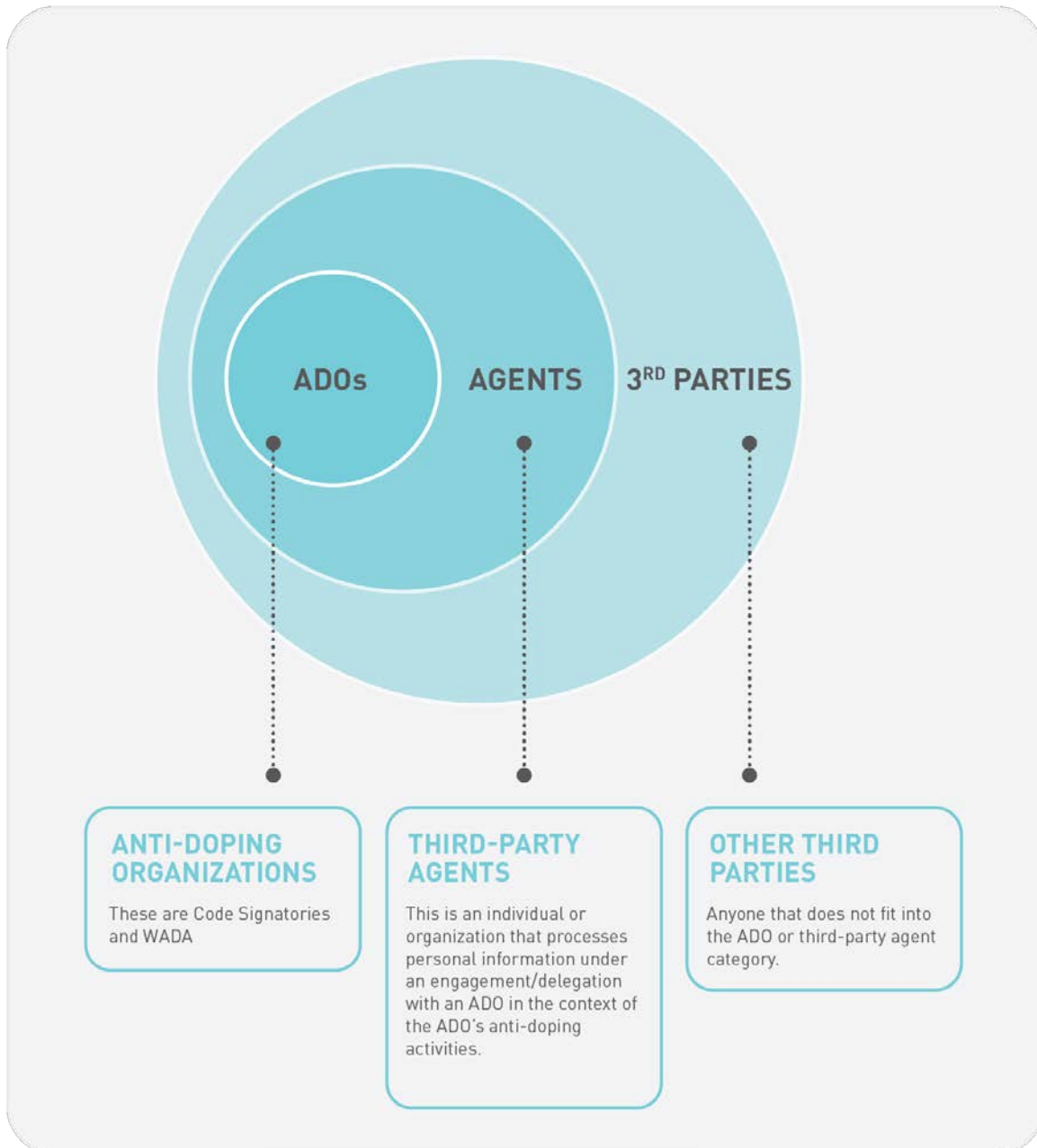
EDUCATING

SECTION 3



1. Identifying and classifying third parties

Before you share personal information, you must understand who you will be sharing it with. The ISPPPI classifies possible recipients into three general categories:



One way to think about these three categories is in terms of circles of trust. As you move from ADOs out to third parties, the conditions for sharing personal information under the ISPPPI become more stringent. This is because you have less control over recipients as you move toward the outer trust circles.

As an ADO sharing personal information with another ADO, you know you are both subject to requirements under the Code and ISs (in particular, the ISPPPI). As you move to third-party agents, you are able - and are required - to impose certain contractual and technical controls to continue to protect personal information in the hands of the recipient. Examples include doping control coordinators, other types of delegated third parties (like national federations, continental federations, or regional anti-doping organizations), experts or consultants or IT service providers. When it comes to other third parties, because you do not have an existing relationship and the recipient will be using personal information for its own purposes, your effective control over this personal information once in the hands of the recipient can be limited. One example of this type of other third party in the anti-doping context is law enforcement.

2. Applying common principles

There are common principles you should apply when sharing any personal information: ensuring there is a need to share, minimizing what is shared, and sharing information securely. In addition, you should bear in mind your obligation to notify individuals in advance of the types of recipients of their personal information (see [Chapter 5: How to explain your processing practices](#) for more).

HOW TO IDENTIFY A NEED-TO-KNOW

When seeking to identify whether a potential recipient has a legitimate need to know the personal information requested, start by identifying the recipient's stated purposes for requesting personal information. Consider whether it is a legitimate purpose considering the recipient's roles and responsibilities (whether as an ADO, a delegate of an ADO, or another third party).

HOW TO MINIMIZE WHAT IS SHARED

If the first criterion is met, you then need to try to minimize the personal information being shared. Consider what type and volume of personal information is strictly needed to achieve the purposes of the request. To do so, do not hesitate to test different scenarios with the recipient:

- ❖ Could they first use a more limited set of personal information (e.g. names) to then tailor the scope of their request for additional types of personal information, ideally relating to a smaller group of individuals?
- ❖ Are you able to simply confirm certain facts that the recipient is interested in, rather than sharing any underlying personal information?
- ❖ Would aggregated or anonymized/redacted information suffice instead?

HOW TO SHARE INFORMATION SECURELY

There are two key aspects of sharing information securely: technical protections and contractual or written commitments.

With respect to technical protections, ADOs should use encryption or a secure file sharing system to transmit personal information electronically, rather than ordinary email. Encryption can be something your email system allows you to enable for specific emails, but also includes simply adding password protection to a document being shared. Secure file sharing systems allow the sender to set access limitations like authentication requirements, expiry dates for access, or download or view limitations. In doubt, consult with your internal or external IT experts to determine what technical protections are available to you.

With respect to contractual or written commitments from the recipients, these can vary greatly depending on the context of your relationship. Consider at a minimum obtaining assurances that personal information will:

- ❖ Be kept confidential and protected;
- ❖ Only be accessed and used for the stated purposes; and
- ❖ Be returned or destroyed when no longer needed.



It is often the case that transferring personal information across international borders is regulated under data protection laws. Where that is the case, you will need to consider what grounds you are relying upon to effect such transfers, which could involve an individual's consent to the transfer, contractual controls, or other measures. In some legal frameworks, such as the EU's GDPR, transfers that serve important public interests are permitted, and these frameworks may, like the EU's, even explicitly identify anti-doping as an important public interest. Similarly, some sport and anti-doping laws expressly permit international transfers for anti-doping purposes. And, in some instances, certain countries with particularly strong data protection regimes, like those in the EU, Canada, or Switzerland, are deemed to provide sufficiently high protections under their domestic laws that it is often possible to transfer data to parties located there. Ultimately, and as stated in the UNESCO Convention Against Doping in Sport, it is vital for anti-doping information to travel across borders given the international nature of sport and for countries having ratified the Convention to implement appropriate measures to provide for this.

3. Sharing with other ADOs

WHAT SHARING OCCURS IN ADAMS?

WADA's Anti-Doping Administration and Management System (ADAMS) was built to facilitate the conduct of anti-doping activities between organizations that have overlapping anti-doping responsibilities with respect to athletes and organizations that are located around the world.

At a high-level, NADOs have access to data related to athletes whose nationality is that of the NADO. IFs have access to data related to athletes associated with the IF's sport. Major Event Organizers (MEOs) have access to data related to athletes participating in events they oversee, for a limited period. ADOs can give third-party agents access to the data they input into ADAMS. WADA has access to ADAMS data to monitor compliance and operate ADAMS. Laboratories can report results to ADAMS while athlete passport management units manage passports in ADAMS.

These sharing rules are based on the division of roles and responsibilities described in the Code and ISs. In these Guidelines, we focus on scenarios that go beyond the sharing rules that are built into ADAMS. For more detail on these rules, see [What information is collected in ADAMS and how is it used and shared?](#) in the [ADAMS Privacy and Security FAQs](#).

HOW TO ASSESS AN AD HOC REQUEST

The ISPPPI permits ADOs to disclose personal information to other ADOs where necessary to allow the recipient ADOs to fulfill their obligations under the Code.

Before sharing personal information with another ADO, the disclosing ADO must be satisfied that:

- ❖ The disclosure is not prohibited by applicable data protection and privacy laws;
- ❖ The recipient ADO has the right, authority, or need to obtain the requested personal information;
- ❖ The requested personal information is only being sent to the identified and relevant person at the recipient ADO;
- ❖ Only personal information that is necessary to the right, authority or need established by the recipient ADO is shared;
- ❖ The mode of communicating the personal information is secure; and
- ❖ There is no reason to believe the disclosure would jeopardize an investigation or the recipient ADO does not comply with the ISPPPI.

In other words, you need to comply with applicable laws, ensure there is a need-to-know, minimize what is shared, and appropriately protect personal information in transit. The requesting ADO can help the disclosing ADO in its assessment by completing the [ADO Disclosure Request Form](#) template. Completing this template will also help the disclosing ADO document its decision for accountability purposes.



NO ADVANCE NOTICE TESTING EXAMPLE

Our earlier example scenario about ABP testing is a good example of an ad hoc need to share personal information between two ADOs. To recap: The NADO has agreed to carry out a certain number of ABP tests when the passport custodian identifies a target testing opportunity within the NADO's territory. For athletes that are not nationals of this partner NADO but who are training or competing within its territory, the NADO would have testing authority but would not have access to the whereabouts needed to locate them for no advance notice testing within ADAMS, and may never have interacted with them before. The NADO asks the passport custodian IF to share certain whereabouts so that the NADO can locate the athletes for testing.

The NADO will use the whereabouts to carry out no advance notice testing in the territory in which it has authority to test. In other words, the purposes of the disclosure are consistent with the purposes for which these whereabouts were collected. The passport custodian IF should ensure the whereabouts details are encrypted (e.g. by adding a password to the document, or sending it via an encrypted link rather than as an ordinary email attachment) and that only the whereabouts related to a specific mission order period, or possible testing window, are provided. The recipient NADO should ensure the document containing the whereabouts is deleted when no longer needed.

WHEN YOU MAY NEED A DATA SHARING AGREEMENT

In cases where ADOs have more established partnerships that involve a regular exchange of information that doesn't occur through ADAMS (and is therefore not covered by the Agreements Governing the Use of ADAMS), you may want to consider establishing a data sharing agreement as a matter of good practice. Examples could be an arrangement to share intelligence or information regarding athlete passports or other types of intelligence information. There is a Collaboration Agreement template for the purpose of the ABP. Among other things, this type of agreement serves to document the assessment of the factors described above within a defined sharing arrangement.

4. Sharing with third-party agents

HOW TO ASSESS A THIRD-PARTY AGENT

In the second trust circle are third-party agents. Even though you will ultimately enter into an agreement or engagement with this agent, these parties are not directly subject to the Code and ISs, and you therefore have less visibility into their policies, processes and practices.

As a result, **before you decide to work with a third-party agent, the ISPPPI mandates that you assess them to ensure that they can provide sufficient guarantees with respect to the technical and organizational measures that will be applied to their processing of personal information.**

To assess your third-party agent's reliability in this respect, make sure you first understand the nature of the services that they will provide, whether they will need access to any of your systems to carry out their duties, and the extent to which they need access to personal information to perform these duties. This follows the common principles discussed above.

Ask questions to your third-party agents and obtain supporting documents to verify their practices. Here are some examples:

- ❖ What are the purposes for which they will use personal information?
- ❖ How will this personal information be collected or accessed, and where and how will it be stored?
- ❖ Can they describe and provide evidence of their privacy program?
- ❖ Can they describe and provide evidence of their information security program?
- ❖ Do they adhere to any security standards or certifications?
- ❖ Do they have processes to identify and assess risks to personal information in their operations?
- ❖ Do they have internal or external audit reports attesting to their practices?
- ❖ Do they have a security breach response plan? Have they experienced a security breach in recent years?
- ❖ Are there individuals or teams assigned to privacy, information security and/or breach response?
- ❖ Do they maintain insurance coverage for information security breaches?

If you work with several third-party agents, a good practice that will also help you demonstrate accountability and compliance with these ISPPPI requirements is to develop a standard assessment survey or questionnaire that you require agents to complete.

You may need to adapt questions to the nature and scope of your proposed engagement with a third-party agent, and have a long and short form, depending on the risks associated with the data processing. For example, if you are working with individual experts, they will likely not have a privacy or information security program. You should still discuss and agree on relevant safeguards the experts should implement to protect personal information in their possession and ensure that they are subject to an express duty of confidentiality. By way of another example, if you are working with individuals like doctors or lawyers, the statutory obligations these individuals are subject to will be relevant to your assessment, as these professionals are often required to protect information received and keep it confidential under applicable professional ethics rules.

WHAT TO INCLUDE IN YOUR CONTRACT?

Once you are clear on the nature and scope of the third-party agent's services and legitimate needs with respect to the collection, use, disclosure or other processing of personal information, you need to document your arrangement in an agreement.

The ISPPPI requires that third-party agents are subject to appropriate controls, including contractual and technical controls, to protect personal information that will be in their custody as part of their engagement with an ADO.

Appropriate contractual controls include provisions requiring that:

- ❖ Third-party agents comply with the ISPPPI and all applicable laws;
- ❖ Third-party agents only process personal information as per the documented instructions of the ADO and not for any other purpose;
- ❖ Any staff handling personal information are subject to a duty of confidentiality;
- ❖ Appropriate technical and organizational security measures are applied to the personal information processed by the agent;
- ❖ Other parties cannot be engaged by the third-party agent to process personal information without prior authorization of the ADO and appropriate contractual controls with those other parties being in place;
- ❖ Third-party agents provide prompt notification and assistance to the ADO where individuals assert rights under the ISPPPI or applicable law, or in the event of a security breach;
- ❖ All personal information be deleted or returned at the conclusion of the service or upon request; and
- ❖ Third-party agents make information available to the ADO to demonstrate compliance with such controls, or otherwise permit the ADO to verify such compliance through audits or other verifications.



ADOs may need to subject third-party agents to specific contractual controls required under applicable law. This will be the case for ADOs subject to the GDPR in their agreements with a third-party agent acting as a “processor” as defined under this law. ADOs should bear in mind that not all third-party agents would necessarily be qualified as a “processor”, and this requires a case-by-case assessment. Many regulatory authorities and advisory bodies have published guidance in this respect. Regardless of the qualification of the third-party agent, appropriate contractual controls should be included in agreements with third-party agents.

ADOs will need to adapt these safeguards to the type of third-party agent and the nature and scope of their engagement. For example, ADOs have a broader duty to ensure that third-party agents that are also delegated third parties under the Code, are subject to a duty of cooperation in the context of any WADA compliance activity. For those working with many agents, it can be helpful to develop a standard set of controls to be included in contracts involving personal information, or a checklist of items that need to be included if you are more likely to use contract templates provided by the third-party.

Appropriate technical controls may include, depending on the nature of the third-party agent's access to the ADO's systems or information:

- ❖ Access restrictions
- ❖ Authentication requirements (i.e. logins, passwords, verification questions, etc.);
- ❖ Encryption, including with respect to any transmitted information; and
- ❖ Logging and monitoring of user access and activities.

If the third-party agent will, as part of an engagement with an ADO, hold or process personal information on their own systems and at their own offices, you should also consider the technical, physical and

environmental measures that will be applied by the third-party agent to these systems and offices (see [Chapter 6: How to protect personal information](#) for details on security safeguards). It is good practice to document any relevant or necessary technical and other controls in your contract. This can be done in many ways, for example by including a schedule specifying relevant controls, or by referring to documentation made available by the third-party agent regarding their own security obligations, or to security standards/certifications maintained by the third-party agents.

The importance of technical controls should not be underestimated. While they are not completely foolproof, they greatly minimize risks associated with human error and malicious attacks. The impact of a human error or third-party attack will be minimized where the relevant human/attacker themselves have limited access to personal information.

TECHNICAL CONTROLS FOR WORKING WITH THIRD-PARTY AGENTS IN ADAMS

When granting access permissions to a third-party agent in ADAMS (they will be called delegated third parties in ADAMS), ADOs are responsible for ensuring these permissions respect the common principles of data minimization and need-to-know.

Controls are available in ADAMS to help ADOs tailor access permissions of their delegated third parties (DTPs). For example, ADOs can:

- ❖ Limit DTP access to specific athletes or non-athletes, or to athlete pools (e.g. RTP) – this limit will apply to all modules the DTP is permitted to access;
- ❖ Select specific modules that DTPs will have access to (e.g. testing, TUE, results management);
- ❖ Set an expiry date for all access permissions; and
- ❖ For DTPs that are sample collection authorities (SCAs), limit access to specific mission orders.

It is strongly recommended that you not allow DTPs to access data related to "All Athletes". Rather, you should select an appropriate subset of athletes (e.g. athletes in your RTP), or create your own athlete groups, to ensure DTP access is limited to what is necessary for their functions.

One common type of DTP in ADAMS is an SCA. If you work with an SCA, you can limit their access permissions to specific mission orders only. Specific mission order access will allow the SCA to access whereabouts information that is limited to the duration of the order, as well as athletes listed on the order, to carry out the relevant doping controls. If you provide a DTP with access to the "testing" module instead, the DTP will have broader access permissions, which includes access to whereabouts for all athletes in the athlete pool you have authorized it to access, and the ability to create and modify test orders and doping control forms.

ADOs should review the guidance provided in the ADAMS Help Center regarding [Delegated Third Party Management](#) for details.

5. Sharing with Other Third Parties

Third parties that are not third-party agents or ADOs sit in the outer trust circle. **Disclosure to this type of party is more strictly regulated under the ISPPPI.** It is permitted only:

- ❖ with informed, express consent of the relevant individual;
- ❖ if required by law, regulation, or a compulsory legal process; or
- ❖ if necessary to assist authorities in the detection, investigation or prosecution of a criminal offence, breach of professional conduct rules, or breach of the Code.

The common principles of ensuring there is a need-to-know, minimizing what is shared, and transmitting information securely also continue to apply. It is good practice to document your assessment of these factors before you share personal information. To do so, you could adapt the [ADO Disclosure Request Form](#) template and use it for requests from other third parties.

DO YOU HAVE CONSENT?

To determine if you have the consent of the individual concerned by the disclosure, consider if you have met the conditions for a valid consent as described in [3. Obtaining valid consent if you need it](#) in [Chapter 5: How to explain your processing practices](#). **The standard here is ‘express’ consent, i.e., it is the same standard as required for sensitive personal information in ISPPPI Article 6.3.** You can also always obtain a specific consent for the disclosure by confirming with the concerned individual that they accept the disclosure at the time you intend to make it.

IS THE SHARING REQUIRED BY LAW, A REGULATION, OR A COMPULSORY LEGAL PROCESS?

You may share personal information with third parties where required by law, regulation, or compulsory legal process. For example, where you are legally obliged to provide information pursuant to a law, statutory instrument, a regulation (including, in limited circumstances, an anti-doping rule regulation), or a court order.

To rely on this provision, you would need to be faced with an obligation to make a disclosure. In other words, just being permitted to make a disclosure or asked to voluntarily make a disclosure would not fit within the scope of this provision.

NATIONAL FEDERATION EXAMPLE

National Federations are not anti-doping organizations. Unless they are working on behalf of an ADO as delegated third party, they will fall under the 'other third party' category under the ISPPPI. National Federations can, however, play a coordination role between ADOs and athletes.

For example, the Code specifies that ADOs may need to inform National Federations of an anti-doping rule violation in advance of public disclosure of a sanction, subject to appropriate confidentiality procedures.

To share personal information with a National Federation for anti-doping purposes, ADOs need to ensure that:

- the NF needs the information in question to fulfil an anti-doping role (e.g. service of documents to an athlete);
- the NF's anti-doping role and the necessary sharing is specified in the ADO's anti-doping rules that are binding on both the ADO and the NF;
- the ADO's anti-doping rules are in conformity with the Code and International Standards (e.g., they must include appropriate procedures for the protection of confidential information).

Taking results management proceedings as an example:

- The NF may only receive results management information in the circumstances permitted by Code Article 14 on the confidentiality and reporting of anti-doping rule violations.
- The NF should only receive necessary information, e.g., a case file should only be provided to an NF if needed to exercise a right of appeal, or if the athlete decides to share this information with the NF.
- Recalling that ADRV proceedings are confidential, and will involve the discussion of personal information, NFs should only be present at a hearing if appearing with the athletes consent or if this presence is necessary to exercise a limited right of appeal as provided for in an ADO's anti-doping rules.

ARE YOU ASSISTING A SPECIFIC AUTHORITY?

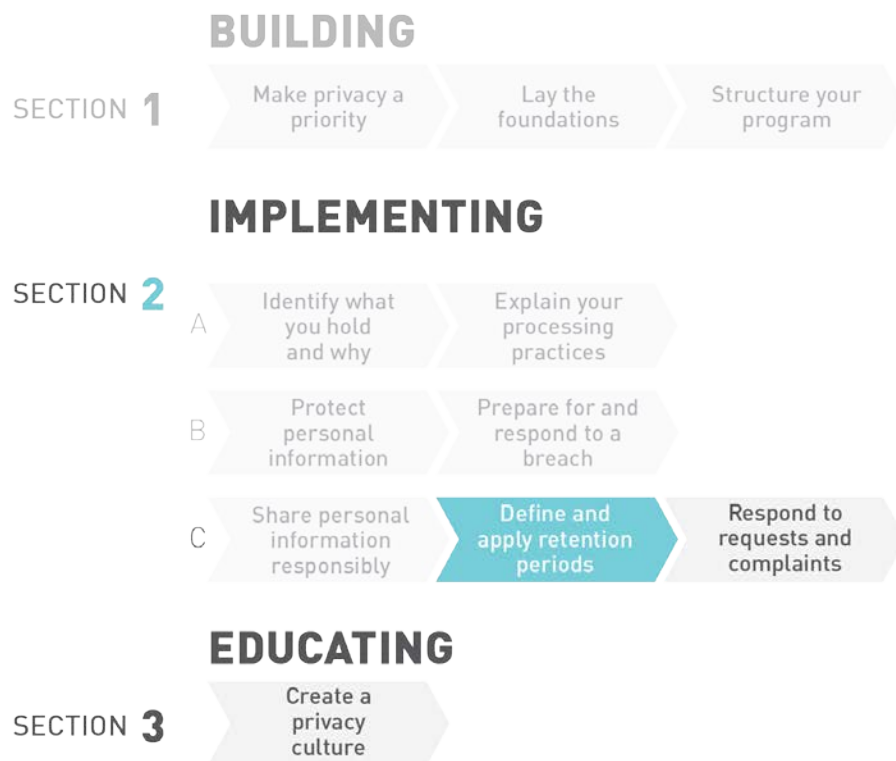
The third possibility for disclosure of personal information is disclosure to law enforcement or governmental or other authorities. **Before you share personal information with this type of entity, you must ensure the following conditions are met:**

- ❖ The disclosure must be necessary to assist in the detection, investigation or prosecution of a criminal offence, breach of a professional code, or breach of the Code;
- ❖ The personal information must be reasonably relevant to the offence or breach in question; and
- ❖ The personal information cannot be reasonably obtained by the relevant authority through other means.

As mentioned in the ISPPPI, sharing personal information with this type of authority may also be regulated under other laws applicable to you. It is possible that applicable anti-doping or sports law encourages or facilitates this type of sharing. It is also possible these same laws or data protection laws contain additional conditions to be met before disclosure can occur.



What personal information should be retained



Retention or storage is a type of processing of personal information. Therefore, the same data minimization principle applies: **Personal information must only be retained to the extent it is relevant to fulfill anti-doping activities or is required by law to be kept.**

1. Understanding Annex A of the ISPPPI

The purpose of Annex A of the ISPPPI is to harmonize retention periods for the main categories of anti-doping data, in the context of key anti-doping activities.

There are now seven modules in Annex A: Athlete profile, Whereabouts, TUE Management, Testing, Test Results, ADRV Proceedings (i.e. Results Management), and ABP. The 'data' column provides more detail

on the types of data included in each module. These data points track the data points that are recorded in ADAMS by all ADOs, for each module. Then, the 'retention period' column provides a maximum retention period as well as the retention trigger for each type of data. The retention trigger determines the starting point for the calculation of the retention period. The 'remarks' column explains why a particular retention period has been set. The 'criteria' column clarifies circumstances where an assessment of proportionality was needed to set an appropriate retention period, in addition to the assessment of the necessity of the data for an anti-doping activity.

The retention of data in ADAMS is mapped to Annex A of the ISPPPI, and data deletion occurs on an automated basis once a retention period has expired. Where Annex A refers to a discretionary ability to extend a retention period, for instance, in the case of a pending or reasonably anticipated ADRV, investigation, or other legal proceedings, the ADO must ensure they keep a copy of the relevant information and hold it outside of ADAMS, or should request that WADA place a hold on information associated with the relevant athlete profile(s) in ADAMS.

See the [How long is ADAMS information retained?](#) page in the ADAMS Help Center for a detailed description of the application of Annex A in ADAMS.

2. Implementing Annex A outside of ADAMS

ADOs must extend the application of Annex A to their own systems and records. Consult your record of processing (see [Chapter 4: How to identify what you hold and why](#)) to identify where documents and records are held and how long they are stored. Assess your answers against the requirements of Annex A under the 2021 ISPPPI to determine where you need to make updates.

Develop specific plans or procedures to ensure personal information is securely retained and eventually deleted, destroyed or anonymized. For retention, this is typically achieved using some form a retention schedule, much like Annex A but adapted to your own systems and filing practices.

At a minimum, retention schedules document record types, retention periods, and some information justifying the retention period (for example, value of the records from a legal, fiscal, administrative or historical perspective, as well as legislative requirements, statutes of limitation, and organizational or archival requirements).

For background, and while this would fall outside the scope of the ISPPPI, retention schedules usually cover all of an organization's record types (not just personal information).

Your record retention schedule will need to be supplemented by information security measures to ensure stored and archived information is protected. If you use software to automate the application of retention periods in your systems, you will likely need processes in place to verify this software is functioning properly. If you have a small organization and will manage retention manually, consider implementing a process whereby the Privacy Manager (or another staff member) confirms that different departments within the ADO have complied with scheduled deletion dates, regularly reviewing such dates, and maintaining a deletion log.

When creating your internal retention schedule, you should consider whether you need to adapt the retention trigger provided in Annex A to a trigger that will allow you to properly operationalize the required retention period in your own systems. Consider the following examples:



ADRV Example (Module 6)

The retention trigger in Annex A for proceedings and decisions related to ADRVs is the 'date of final decision'. In ADAMS, the operative date will generally be either the date of the first instance decision, or, where there is an appeal, the date of the decision on the appeal. In your own filing system or database, you may label a case as final using another term, such as 'case closed'. In these circumstances, you will need to program your system, or provide instructions if you have a manual deletion process indicating that for your purposes, 'date of final decision' means date a case is labelled 'case closed'.



Athlete Profile Example (Module 1)

The retention trigger in Annex A for athlete profile information is either the exclusion from an ADO's testing program or the moment other data categories have been deleted, whichever is later. Focussing on the first case, the operative date in ADAMS is the date of the last test. It is a rolling trigger, meaning that it will be regularly updated - deletion would only occur when the last test date associated with an athlete profile is 10 years old. This date was chosen because it can be consistently applied for all ADOs that use ADAMS. In your own filing system or database, you may have specific records identifying the date of an athlete's inclusion or exclusion in a testing pool, which directly aligns with the Annex A retention trigger, or you may need to use another date, like date of retirement, or date of last test as in ADAMS, as the equivalent date in your systems for the date of exclusion from a testing program. The important thing is to choose a retention trigger that you can consistently apply across your systems and databases, and that aligns with the retention trigger under Annex A.

You should also note that Annex A has a built-in grace period of a calendar quarter for the deletion of data once a retention period has expired. This grace period is intended to facilitate the implementation of Annex A into ADO's own systems or as part of a manual review/deletion process.

3. Defining retention periods for other data

For personal information processed by ADOs, but not covered by Annex A, ADOs must respect the retention principles of ISPPPI Article 10, i.e. retaining personal information only where relevant to an anti-doping activity or as required by law. You must take into account the purposes for which personal information is processed to assess the relevance or need for its retention (e.g. TUE management, whereabouts, testing, etc.). Moreover, where sensitive personal information is involved, the ‘relevance’ criteria must be narrowly interpreted. In other words, more compelling reasons are needed to retain sensitive personal information.

You are encouraged to define specific retention periods for any personal information not covered by Annex A, based on the above retention criteria, and to document these periods in a retention schedule or process. When deciding the length of time for which any information will be retained, consider the following questions:

- ❖ What is the internal organizational need to keep the information?
- ❖ Are there any regulatory requirements mandating the retention of the data and, if so, what do they provide for?
- ❖ Are there any relevant legal statutes of limitation, or would the information be necessary in any pending or imminent litigation?
- ❖ Is the information needed to meet applicable legal reporting needs?

4. Deleting, destroying or anonymizing when retention periods expire

Once personal information is no longer needed to fulfill obligations under the Code or ISs, or no longer needed to be kept by law, the ISPPPI requires that it be deleted, destroyed, or anonymized.

‘Destruction’ typically refers to records stored in a physical form, such as paper documents or electronic data held on physical archive tapes. Different techniques can be used to physically destroy records.

For example, you can destroy paper records by shredding them and ensuring the shredded documents are then disposed of securely by a trusted provider. Paper records containing personal information should not be placed in ordinary recycling or garbage. You can destroy physical tapes through incineration or degaussing (a process that scrambles – i.e., destroys - data on a tape by exposing it to a magnetic field). Specialized record management providers can assist you with the secure destruction of physical records.

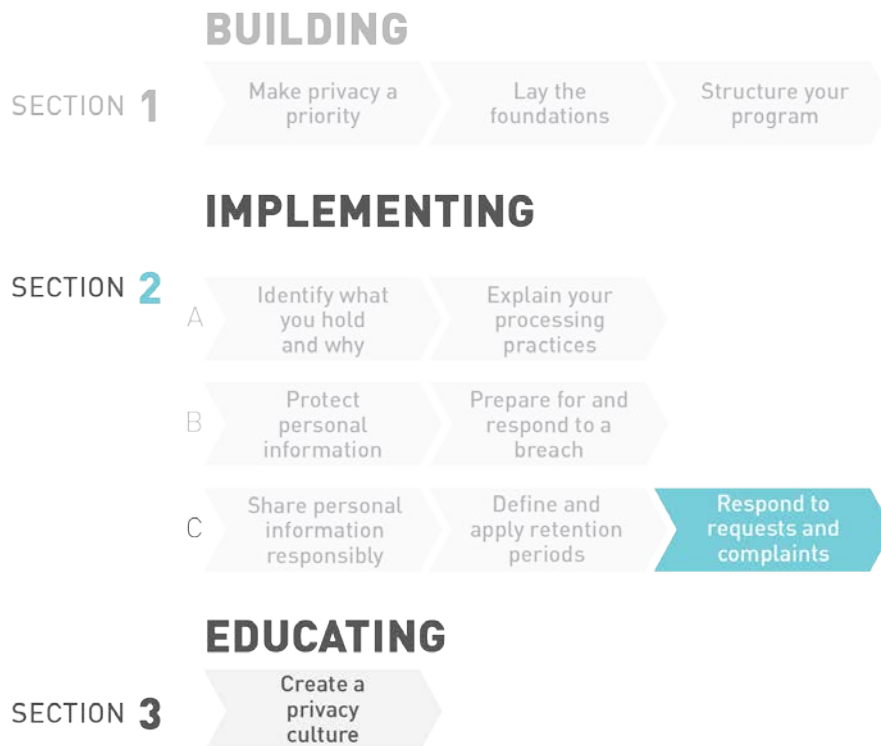
‘Deletion’ and ‘anonymization’ typically refer to records stored in electronic form. Electronic deletion is more complex than physical destruction, because electronic data will likely exist at multiple system and application layers. Assistance from IT professionals is recommended to review and assess your electronic deletion processes.

The standard of anonymization required under the ISPPPI for continued storage of data once it is no longer needed for anti-doping activities (in identifiable form) and no longer required to be held under applicable law is 'permanent' anonymization. This means that individuals can no longer be identified in the data, and the means used to render the data anonymous cannot be reversed to re-identify such individuals. This can be a useful and more appropriate tool than data deletion where the anonymous data still has value for an anti-doping organization but is no longer needed in an identifiable form. For example, statistics on testing or ADRVs are created from identifiable records, but personal information has been removed. They continue to have historical, scientific, and educational value in aggregate form.



To ensure systems containing personal information are resilient and can be restored quickly, it is important that they are backed-up or archived separate from the primary system and often in a remote location. This can result in information being retained, even after it has been deleted or wiped from the primary system, for longer periods of time. Depending on applicable laws, it may be the case that information placed in secure, archived systems will be permitted to be retained for longer periods. ADOs should consider any pertinent regulatory guidance from their national authority.

How to respond to requests and complaints



1. Understanding individual rights regarding personal information

Individuals have rights concerning the processing of their personal information under the ISPPPI.

This is related to the individual participation principle. In this Chapter, we first look at different types of rights, and then review processes to follow when responding to a request or complaint.

RIGHT TO ACCESS INFORMATION

Individuals have the right to receive the following from ADOs:

- ❖ Confirmation of whether the ADO processes personal information relating to them;
- ❖ The information required to be included in an ADO's privacy notice per ISPPPI Article 7.1 (see [Chapter 5: How to explain your processing practices](#)); and
- ❖ A copy of requested personal information in the possession of the ADO.



Although the ISPPPI reflects most of the rights that exist under data protection and privacy laws, ADOs should review relevant legislation (including sports and anti-doping legislation) and regulatory guidance to better understand how these rights are applied in their jurisdictions, and to determine whether any additional rights or exceptions exist. Under the EU GDPR for example, individuals have a right to not be subject to purely automated decision-making having legal or equivalent effects, unless it is needed to perform a contract, is authorized by law or takes place with consent.

If individuals have additional rights that are not provided for under the ISPPPI or are required to follow any specific processes to exercise them under applicable data protection and privacy laws, it would be good practice to add this information to your privacy notice. This would be an example of additional information being provided under Article 7.1 to ensure the processing of personal information remains fair to individuals. For instance, where individuals have the right to file complaints with a national data protection regulator, you should inform individuals of this.

RIGHT TO CORRECT OR LIMIT PROCESSING

Individuals can request that an ADO rectify, amend, block, or delete personal information if an ADO's processing of that personal information is shown to be inaccurate, incomplete or excessive.

An example of excessive processing would be processing that is not necessary or fails to serve any legitimate anti-doping activity. Inaccuracy or incompleteness would typically be found in the personal information itself, rather than in any processing operations.

RIGHT TO REFUSE OR WITHDRAW CONSENT

Where ADOs rely on consent to process personal information, a person may refuse to grant or withdraw consent to the processing of his or her personal information at any time. This right is addressed in ISPPPI Article 6.2, rather than ISPPPI Article 11. The impact of exercising this type of right is similar in practice to a request to block or delete personal information.

As mentioned in [3. Obtaining valid consent if you need it](#) in [Chapter 5: How to explain your processing practices](#), individuals should be informed in advance of the circumstances where an ADO would still need to process personal information despite a request to block, delete, or withdraw consent. Similarly, individuals should be informed of the consequences of refusing to consent, or blocking/deleting personal information, in the anti-doping context (e.g. possible ADRV or disqualification from sporting events).

RIGHT TO SUBMIT A COMPLAINT

Individuals can file a complaint with an ADO if they believe that their personal information is not being processed in accordance with the ISPPPI or applicable data protection and privacy laws.

Complaints can be tied to the types of rights requests described above, or could be linked to questions about the ADO's other personal information processing practices, policies or procedures.

If the individual believes that the ADO has not satisfactorily resolved the issue, they may notify WADA at compliance@wada-ama.org or privacy@wada-ama.org. WADA will treat the notice in accordance with the International Standard for Compliance by Signatories (ISCCS).

2. Responding to a request or complaint

Now that you understand the types of rights available to individuals under the ISPPPI, let's review the key response steps. It will be helpful for you to document these steps in a policy or procedure in a way that is adapted to your organization. The ISPPPI only requires that you have a documented process to respond to complaints, but it would be more efficient to create a process to respond to all types of privacy requests or complaints. This process will help you demonstrate accountability and compliance under the ISPPPI.

HOW TO IDENTIFY THE TYPE OF REQUEST OR COMPLAINT

Ideally, individuals who have requests or complaints will direct them to your Privacy Manager, using the contact information you provided in your privacy notice (see [Chapter 5: How to explain your processing practices](#)).

It is possible, however, that someone else in your organization could receive a request or complaint under the ISPPPI. It is also possible (and in fact, likely), that the individual requester will not formally or expressly invoke their 'right to obtain a copy' or to 'access personal information' or to 'correct or limit' the processing of their personal information.

If someone requests that documents containing personal information be provided to them, or challenges the accuracy or completeness of personal information, this should be regarded as a request to exercise the types of rights described above. You could also receive requests verbally, especially if you make help or support phone lines available to individuals (note that some jurisdictions require that rights requests be made in writing).

The Privacy Manager should make sure that staff, especially staff with frequent interactions with athletes and others, are aware of the possibility that they may receive this type of request or complaint and are trained to direct these to the Privacy Manager. If you do receive verbal requests, it is good practice to document the request in writing for your own records.

If you have the resources and receive a high volume of requests, there are privacy vendors that offer solutions to manage the processing of these requests. These solutions have the benefit of being customizable to privacy and data protection laws applicable to you. They typically also involve creating a standard form that individuals can complete to provide you with the information you need to properly classify and respond to a request. Always remember, however, that you typically cannot require individuals to use a specific form or procedure to send you a request to exercise their privacy rights.

WHAT TO INCLUDE IN YOUR ACKNOWLEDGMENT OF RECEIPT?

After identification of the type of request or complaint, the first step in responding is to acknowledge receipt. It is good practice to communicate to the requester that their message was well received and will be handled by you.

This is also a good time to ask any follow-up questions you need to properly understand the nature and scope of the request and/or verify the identity of the requester. It is important to assess if you need any more information from the requester within a few days of receiving of a request, so that you can receive these details in good time and still respect the time limits in which you need to respond.

Consider the following questions:

- ❖ Do you need to confirm the identity of the requester?
- ❖ Is someone making a request on another person's behalf? If so, do you need to confirm their authority to act for this other person?
- ❖ Is the request clear? Do you understand what the individual is asking for?
- ❖ Is the request very broad? If so, you can ask the requester to clarify the nature and scope of his/her request.
- ❖ Is the information the requester is asking for in your possession, or should they be re-directed to another organization?
- ❖ Is the request directed to several recipients?
- ❖ Is the request made in the context of a results management process?
- ❖ Is the request made in the context of or related to an ongoing investigation?

HOW TO VERIFY THE IDENTITY OF THE REQUESTER

You have the responsibility to ensure you are not providing personal information to the wrong person or editing or amending personal information without the consent of the right person. This is important to protect personal information against unauthorized access.

You may therefore need to confirm the identity of the requestor before complying with their request. That said, there are circumstances where this may not be needed. For example, if an individual is merely seeking

general information about your privacy practices, there is no need for him or her to identify themselves to you – you can simply respond with the requested general information.

If you do need to confirm an individual's identity, this can be done in different ways. As always, you should only request the personal information necessary to identify the requester.

For instance, you could ask for a few personal details that you can then confirm in your system (e.g. an ADAMS or other unique ID combined with a person's name and date of birth). If you do request a copy of an identification document (like a driver's license or passport), or if an individual proactively provides this with their request, it is good practice to delete this copy once you have completed your verification. You can document, for your records, that the person identified themselves by providing a copy of their ID. You should also provide a secure means for the individual to provide this copy to you (for example, an upload link or other encrypted channel).

If you receive a request from a third-party acting on behalf of an individual, they will need to confirm their authority to act for that individual. You will also still need to confirm the identity of the individual who is the subject of the request. Often, this will be a lawyer acting on behalf of a client, but it could also be a parent acting on behalf of a child, or a family member, coach, or another person that an individual has mandated to act for them. Again, you should always adapt to the circumstances to conduct this verification.

Examples of ways to confirm this authority are:

- ❖ Asking for a general or specific power of attorney or other letter of authorization;
- ❖ Confirming the delegated authority directly with the individual that is the subject of the request;
- ❖ Establishing through existing documentation in your possession that the person has appropriate authorization to make the request; or
- ❖ Verifying your records to confirm that a person is indeed the parent of a minor athlete and confirming their identity.

HOW TO GATHER INFORMATION FOR YOUR RESPONSE

The type of search you need to conduct will again depend on the type of request. If it is a very specific request for access or for correction, your search will be limited. If you receive a request for a broad range of data, then you may need to conduct multiple searches across different systems. It may be helpful here to clarify the scope of the request with the requester.



When in doubt, consult regulatory guidance to better understand what you are expected to do to gather information in response to a request. In practice, regulators will expect organizations to expend reasonable efforts to locate any responsive information, but generally do not expect them to uncover every possible stone in the off chance that it might lead to some additional information being located.

It will also be helpful for you to understand, in advance, how your different systems or databases can be searched. For example, are you able to pull all records associated with a name or ID? Is your search capability more limited? How much work would be required if you needed to respond to a broad request for a copy of personal information?

Remember, in this context, that you can extract records associated with an ADAMS ID using the ADAMS' reporting functions.

WHAT EXCEPTIONS SHOULD BE CONSIDERED AND APPLIED

There are limits to privacy-related requests and complaints, both under the ISPPPI and applicable laws. Also, you should bear in mind other interests, including third-party confidentiality interests and public interests when responding to requests, particularly access or deletion requests.

First, if the request relates to or seeks information other than personal information (for instance, organizational minutes, or general statistics), this is not a request that is subject to the ISPPPI (or to privacy and data protection laws).

Assuming the request concerns personal information, consider if any of these exceptions apply:

- ❖ If you are providing a copy of personal information, does it contain personal information about another person (note that opinions can be the personal information of both the person emitting the opinion, and the person that is the subject of that opinion)? If so, can you still fulfil the request while redacting the personal information of the third party?
- ❖ Does complying with the request conflict with your ability to conduct no advance notice testing, or to investigate or establish an ADRV or another legal claim?
- ❖ Does the request otherwise conflict with the aim of maintaining the integrity of the anti-doping system?
- ❖ Does the request impose a disproportionate burden on the ADO in terms of cost or effort, given the nature of the personal information requested?

Some of these exceptions are discretionary and require a careful, case-by-case assessment that should be documented. Documenting your assessment will help you in the event a regulatory authority, or WADA, as part of a compliance monitoring process, asks you to provide your justifications for any refusal to act on a request. In the anti-doping context, examples of where these exceptions may apply include:

- ❖ A request to delete personal information relevant to an active or imminent ADRV investigation or process;
- ❖ A request to restrict processing of personal information where this processing is needed to conduct an anti-doping activity (e.g. a mandatory doping control process); or

- ❖ Circumstances where law enforcement or other authorities have indicated that fulfilling a request for personal information would hinder their investigation into a breach of an applicable law.



When considering whether any exceptions apply, and how to apply them, ADOs should look to applicable laws (including sports and anti-doping laws) and regulatory guidance. For example, frequent exceptions to the right to access personal information under data protection laws include circumstances where providing the information may: harm the rights and interests of organizations by disclosing trade secrets and other sensitive business information; or result in the disclosure of legally privileged material.

HOW LONG DO YOU HAVE TO RESPOND?

You should normally respond to a privacy-related request or complaint within 30 days, or four weeks, of receiving a properly formulated request.

'Properly formulated' means that you have been able to confirm the identity of the request (and authority of any third party, where relevant), and to obtain any reasonably required clarifications from the requester to fulfil the request.

'Responding' in this context also means providing a substantive response, i.e. either fulfilling the request or providing reasons for the refusal.

If the amount of personal information at issue is significant, and if assembling it will require a disproportionate effort, your response may legitimately be delayed beyond 30 days. Where this is the case, you should inform the individual of the delay, explain the reasons for it, and provide a revised time estimate for the response before the first 30 days have expired.



Note that extending the timeframe beyond 30 days requires a strong justification and should only occur in a minority of cases with documented reasons. You should also note that applicable laws may impose a maximum time limit for this type of delay (e.g. an additional 60 days). If you can, you could also provide information on a phased basis, meaning some more readily accessible information could be provided sooner than other information.

WHAT TO INCLUDE IN YOUR RESPONSE?

Your response must include the following minimum information:

- ❖ If you are fulfilling the request, in full or in part, confirmation that you are doing so along with any relevant supporting documentation (for example, a copy of the requested personal information, or evidence that a requested correction has been completed); and
- ❖ If you are refusing to fulfil the request, in full or in part, the reasons for the refusal.

If you are providing a copy of personal information, also keep in mind:

- ❖ Do so using secure means, like an encrypted document or a file sharing service; and
- ❖ The information should be in a format that is intelligible to the individual (i.e., if there are many labels or codes associated with the data - this can be the case for electronic data pulled from a database, you may need to explain these labels or codes to the individual - e.g., “1” means yes and “0” means no, or not applicable).

CAN YOU CHARGE FEES?

You should typically fulfil this type of request at no cost to the individual. Applicable laws may permit organizations to charge nominal fees for things like printing costs, if relevant. Under the ISPPPI, these costs should not be excessive. If you are charging this type of fee, you should advise the requesting individual in advance.

SHOULD YOU NOTIFY ANY OTHER ORGANIZATIONS?

If you make a correction, delete information, or agree to restrict the processing of personal information, you must inform the other ADOs that have access to or process this information, unless this proves impossible or involves a disproportionate effort.

Before you take the lead in responding to a request, you should also consider if another organization would be better placed to respond to it. In this regard, the ISPPPI provides that the ADO that has the primary relationship with the athlete (for example, the NADO in the case of a national-level athlete, or the IF in the case of an international-level athlete) will typically be responsible for responding to privacy-related requests or complaints from this athlete. To provide a simple example, if an athlete has a question or request about their biological passport, the passport custodian is likely best placed to respond.

If another organization holds personal information on this same athlete and receives a request, they can also choose to respond. In WADA’s case, we will typically correspond or coordinate with the ADO responsible for a particular athlete, unless it would be inappropriate in the circumstances (for instance, if the athlete requests confidentiality in their request).

SECTION 3:

Educating staff on your privacy program

Section 3 includes Chapter 11. This section will provide support for all Articles by helping you make sure every person in your organization understands and applies the requirements of your privacy program. Creating a privacy culture and training staff is itself a key security safeguard for personal information.



How to create a privacy culture

BUILDING

SECTION 1



IMPLEMENTING

SECTION 2



EDUCATING

SECTION 3



You will know you have succeeded in creating a privacy culture when applying privacy principles to day-to-day anti-doping activities becomes second nature for every person in your organization. You will also find that compliance with the ISPPPI and with privacy and data protection laws is one of the many benefits of your successful privacy program, rather than your key focus.

In Section 1, we discussed the importance of getting buy-in from top management for your program and building privacy into your organization’s governance structures. That is the first building block of creating a privacy culture. In this section, we will focus on two other building blocks: creating privacy champions and engaging all staff in the creation of your privacy culture.

1. Training your privacy champions

The Privacy Manager you are required to appoint under the ISPPPI is your main privacy champion. If you are a larger organization, you can also consider creating privacy champions in key operational areas of your organization, for example, in testing or results management.

Investing in training for your privacy champions will help you multiply the strength of your privacy program, as these individuals use and share their expertise across the organization.

There are many free and cost-efficient resources to help train privacy experts. For example, the International Association of Privacy Professionals (IAPP) brings together privacy professionals from around the world. Members can access guides, templates, webinars and other resources. The IAPP also offers various certification programs for privacy professionals. Several companies also provide research and privacy news platforms on a subscription basis. The IAPP publishes an annual Privacy Tech Vendor Report where you can find many of these platforms and determine if they are right for you.

2. Training your staff & raising awareness

Now that you have your privacy champion(s), training the rest of your staff is the next step. Not only is this a key step in creating a privacy culture, it is also a key safeguard for personal information, and should feature within your privacy and information security programs.

The ISPPPI requires that staff that have access to personal information be informed of the need to keep personal information in confidence. Similarly, ADOs commit to ensuring staff have received appropriate privacy and security training in the agreement governing the use of ADAMS.

There are many ways you could achieve this objective, and many tools exist to help you, starting with free courses and webinars available on ADEL.

Use the Privacy Tech Vendor Report mentioned above to identify eLearning providers. Many eLearning providers specialize in information security and privacy training content and can offer you a large library of courses to choose from. They can also offer you access to a learning management system (LMS) that will allow you to easily assess knowledge, assign courses to your staff and track completion. Some tools also offer additional reinforcement learning tools like the ability to create and send phishing simulations.

You can combine these eLearning tools with live/in-person training from your Privacy Manager. If you already provide information security training, consider combining your efforts to deliver a training program covering both privacy and security. Privacy Managers should also consider partnering with education managers and Human Resources staff that have expertise in education and may already have tools available for privacy training.

Whatever tools and formats you choose for your privacy program training, we recommend you incorporate the means of assessing knowledge gaps, train regularly, and measure your progress.

HOW TO ASSESS KNOWLEDGE AND IDENTIFY GAPS

Assessing existing knowledge will help you provide more relevant training content to your staff. Before you start your assessment, consider:

- ❖ How many staff do you need to educate?
- ❖ How do they typically receive information about organizational policies and codes of conduct?
- ❖ What types of roles exist within your organization?
- ❖ How many staff access and use personal information regularly?
- ❖ What tools do staff use most often to complete their work (e.g. word, excel, third-party platforms, etc.)?
- ❖ What types of privacy or information security training have your staff has received in the past?
- ❖ What is the general technical literacy within your organization?

Use the answers to these preliminary questions to develop your assessment questions and start thinking about your training content. To deliver these questions, you could use tools like a survey or an assessment tool built into your LMS. You can also find survey templates online.

A phishing simulation tool can also be useful to assess knowledge and understanding of phishing threats. These tools can be integrated directly in your email system and will help you identify employees that need further training.

WHAT TO INCLUDE IN YOUR TRAINING PROGRAM?

To help ensure privacy training is prioritized by your staff, we recommend making at least minimum aspects of your program a mandatory training requirement. This will help provide you with the information you need to measure the impact of your efforts.

When developing or purchasing training content, consider if your training program covers topics like:

- ❖ Relevant legal requirements, regulatory authority guidance, and industry standards;
- ❖ Information about legal and reputational risks relevant to your organization's functions;
- ❖ An overview of relevant policies and procedures;
- ❖ Information about the organizational, technical, physical and environmental safeguards in place to protect personal information;
- ❖ Information about common cyber threats, how to spot them and how to protect against them; and
- ❖ Information about how to respond to a security breach.

Also consider if the training content will help close the knowledge gaps identified in your assessment. If your assessment revealed greater education needs for certain groups, consider providing these groups with additional content or training activities. Larger organizations should also consider providing role-based training for groups with specialized needs or functions. For instance, a TUE Manager must be trained on handling highly sensitive data. An Education Manager dealing with low sensitivity data will not have the same need.

HOW TO MEASURE PROGRESS AND REINFORCE LEARNING

As for any education program, it is important to document the activities you undertake and measure the impact of your efforts. Making sure at least some of your training content includes assessment questions will help you do this. If you use an LMS, you are likely equipped with the tools to track training completion and scores. You can use these measures to identify learners who need additional training to reinforce their learning.

These tools can also be a gateway to integrating games or incentives to your training program (for example, you can award prizes to top scoring staff or departments).

If you do not have assessment tools built into your training content, you can easily plan to carry out your own assessments on a regular basis, using the assessment strategies described above. Over time, this will help you identify trends and progress.

Beyond formal training, take every opportunity you can to raise awareness about privacy matters and reinforce learning. This can be done in different ways. It can be as simple as including privacy in your employee handbook or onboarding process. It could also involve periodic awareness emails, or sharing an article or resource discussing privacy matters with a colleague.

The phishing tool mentioned earlier is also a great tool for reinforcement learning. You can encourage employees to report potential phishing emails and use the opportunity to engage with your staff about why they were correct (or not) in reporting the email.

