European Data Protection Board

Recommendations

Recommendations 1/2025 on the 2027 WADA World Anti-Doping Code

Adopted on 11 February 2025

Executive Summary

By way of letter dated 2nd October 2024[1], the European Commission (Directorate-General for Education, Youth, Sport and Culture) requested the EDPB pursuant to Art. 70 (1) (e) GDPR to examine the current update of the World Anti-Doping Code (hereinafter the 'Code') and its complementing International Standards (hereinafter the 'Standards') in order to assess their compliance with the GDPR. In 2023, the World Anti-Doping Association (hereinafter 'WADA') launched a revision of the Code and its Standards, to be concluded by December 2025, and to come into effect in January 2027. The Code aims at harmonising anti-doping policies, rules and regulations internationally and it is complemented by eight International Standards with the objective of fostering consistency among anti-doping programmes that are implemented mainly via the National Anti-Doping Organisations (hereinafter the '(N)ADOs'). The eight International Standards refer to the following aspects: data protection; education; intelligence and investigations; laboratories; results management; testing; therapeutic use exemptions; and compliance.

The EDPB and its predecessor, the Article 29 Working Party (hereinafter the 'Art. 29 WP'), have attentively followed WADA activities over time, when reviewing earlier version of the Code and its Standards. The Art. 29 WP adopted two Opinions in 2008[2] and 2009[3] on certain provisions of the Code and its International Standards. Subsequently, in 2013, the Art. 29 WP sent a letter to WADA[4] containing a number of observations and concerns regarding the update of these documents. Lastly, in 2019, the EDPB provided its remarks regarding the (at the time ongoing) revision process of the Code and its Standards in a letter addressed to the Presidency of the Council of the EU[5].

The EDPB recalls that the rules of the Code and its Standards have been transposed by Member States into their national legal order, according to their respective national structure and organisation of sport. Indeed, as signatories to the 2005 UNESCO International Anti-Doping Convention and the Anti-Doping Convention of the Council of Europe, Member States have to adhere to the commitments arising from the ratification of these conventions.

---

[1] European Commission, Request for examination of the draft revised World Anti-Doping Code and the relevant Standards referring to data protection (Ref. Ares (2024)7027092 - 03/10/2024)

[2] Art. 29 WP, Opinion 3/2008 on the World Anti-Doping Code Draft International Standard for the Protection of Privacy, adopted on 1 August 2008, WP 156.

[3] Art. 29 WP, Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations adopted on 6 April 2009, WP 162.

[4] Letter sent by the Chair of the Art. 29 WP to WADA on 5 March 2013 and its Annex (Ref. Ares (2013)289160 - 05/03/2013).

[5] Letter sent by the Chair of the EDPB to the Presidency of the Council of the EU on 9 October 2019 (Ref: OUT2019-0035).

As clarified by the Opinion of the Advocate General in the case C-115/22[6], although the Code is a private legal instrument, its effectiveness is ensured by the 2005 UNESCO International Anti-Doping Convention. Per Article 4 thereof, the provisions of the Code are not an integral part of the Convention and do not have direct effect in national law. However, by the same provision, the Member States, which are Parties to the Convention, have committed to abide by the principles of the Code. That commitment is transposed into the legal systems of the Member States in different ways, since, as specified by a 2017 study conducted for the European Commission[7], the Code is legally binding in some Member States, but not in others.

In any case, the EDPB reminds that when Member States adopt national anti-doping measures, encompassing legislation, regulation, policies or administrative practices, based on the principles of the Code, they have to ensure that those measures are in line with EEA law, including the GDPR. Therefore, in case the provisions of the Code and its International Standards are not in line with the GDPR, Member States cannot transpose them as they stand into national anti-doping measures, without infringing their obligations under EU/EEA law and thus negatively affecting the level of protection of natural persons in the EEA with regard to their personal data[8].

Moreover, anti-doping programmes are mainly executed by (N)ADOs, which are among the signatories to the Code. (N)ADOs have to apply anti-doping measures that Member States establish in line with their commitments under the International Anti-Doping Convention and in response to expectations from WADA. The EDPB emphasises in this regard that in the implementation of the national anti-doping measures, (N)ADOs as controllers, are responsible for processing personal data in compliance with the GDPR and, as administrative authorities[9] must not apply, if necessary, those national anti-doping rules in so far as they may be contrary to provisions of the GDPR that have direct effect[10]. Therefore, Member States, when implementing national anti-doping legislation, regulation, policies or administrative practices, should carefully assess whether the provisions of the Code and its International Standards entailing the processing of personal data are compatible with the GDPR so as to also avoid possible infringements of EEA law by (N)ADOs, and any exposure to the corrective actions and sanctions of the competent data protection authorities.

[6] See Opinion of Advocate General Ćapeta delivered on 14 September 2023 in the Case C-115/22, ECLI:EU:C:2023:676, paragraph 5.

[7] Anti-Doping & Data Protection. An evaluation of the anti-doping laws and practices in the EU Member States in light of the General Data Protection Regulation, Study carried out for the European Commission by the Tilburg Institute for Law, Technology and Society of the Tilburg University and Spark Legal, Luxembourg, 2017

[8] See to that end: Judgement of the Court of Justice of 3 September 2008, Joined cases C-402/05 P and C-415/05 P, *Al Barakaat,* ECLI:EU:C:2008:461, paragraphs 281-285.

[9] According to the 2017 study conducted for the European Commission referred to in the above footnote 8, the majority of N(ADO)s are public bodies, usually either established by law or by government.

[10] See lastly and mutatis mutandis, Judgement of the Court of Justice of 7 May 2024, *NADA e.a.,* C-115/22, ECLI:EU:C:2024:384, paragraph 55.

In its Recommendations, the EDPB shares some points of concern with the European Commission regarding the main aspects of the current revision of the Code and its Standards that are not in line with the GDPR, thus negatively affecting the Member States obligation to ensure a consistent and high level of protection to the rights and freedoms of natural persons in the EEA, in particular with regard to their rights to privacy and the protection of personal data. The EDPB will focus on the most important issues and the new concepts introduced by WADA in the International Standard for Data Protection (hereinafter 'ISDP'), as mentioned in the European Commission request and will refer to its letter of 2019 for aspects that relate to its previous findings. Even if not all the relevant provisions of the other Standards complementing the Code are mentioned, they should be considered as having been referred to in these Recommendations as the EDPB remarks may still apply to them.

The EDPB welcomes the changes and progress made in the Code and its International Standards, noting that some of the issues referred to in the EDPB letter dated 9 October 2019 have been successfully resolved, such as setting a stricter deadline for notification of security breaches, and the requirement to carry out a data protection impact assessment prior to processing due to the newly introduced principle of privacy by design[11].

The EDPB welcomes the addition of the International Standards for Intelligence and Investigations (hereinafter the 'ISII'), as part of the overarching WADA standards, as the processing of personal data for investigative purposes is a key activity of (N)ADOs.

However, the EDPB notes that unfortunately certain key issues have not been taken into account when revising the Code and its Standards. In particular, the EDPB still raises doubts about compliance with the GDPR concerning the legal basis of consent foreseen by the ISDP, as in line with Articles 5(1)(a), 6(1)(a), 7, 9(2)(a) of the GDPR, consent must be freely given and the refusal to provide consent, or its withdrawal, can be seen to have a detrimental or adverse outcome for the data subject.

In addition to this, the EDPB notes that the purposes for certain processing activities remain vague. The principle of purpose limitation, under Article 5(1)(b) of the GDPR requires that personal data be processed only for specific, explicit and legitimate purposes. A consequence of this, is that the corresponding retention periods for personal data therefore lack a clear justification.

The EDPB notes that the roles of WADA and (N)ADOs with regard to data processing activities, particularly within the database of the Anti-Doping Administration and Management system (hereinafter 'ADAMS') remain unclear. This not only affects how data protection responsibilities are assigned and managed, but also has an impact on transparency, accountability, and the ability of data subjects to effectively exercise their rights.

[11] See Sections 5.1.and 10.4 of the ISDP.

Additionally, the legally binding nature of the Code for those bodies that have signed up to it should be made explicitly clear. Moreover, the reuse of samples, and personal data including health data should be subject to appropriate safeguards to protect the rights and freedoms of data subjects. Additionally, the purposes for analysing biological samples should be more precisely identified.

The safeguards provided for all data processing under the Code should be equivalent to the standard required by the right to data protection as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union and in the GDPR. Even though the EDPB understands that the Code covers international data flows, national applicable provisions that offer a lower level of data protection should not undermine the safeguards provided for by the Code and Standards.

The EDPB invites the European Commission to encourage WADA to incorporate the EDPB's feedback to make their Code a global Standard of data processing in compliance with the highest level of protection of the fundamental rights and freedoms of all individuals concerned.

Table of contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC], (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[12],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING RECOMMENDATION:

1. Scope and legally binding nature of the Code

1. The EDPB finds that the concerns expressed in its letter of 2019 regarding the scope of the Code, particularly the discretion for (N)ADOs to extend the applicability of anti-doping rules to recreational athletes, thus bringing them within the scope of the Code, remain valid[13]. In this regard, the EDPB reiterates that, in light of the principles of proportionality, necessity and data minimisation, extending the scope of the Code and its International Standards to athletes on a recreational level (i.e. those who engage in recreational sporting activities but not formal competition) would constitute a disproportionate interference with the right to privacy and to the protection of personal data of the concerned persons.

2. Furthermore, according to Sections 1.0 and 4.0, the ISDP only set forth "a minimum, common set of rules", to which (N)ADOs and other relevant stakeholders must conform when processing personal data pursuant to the Code. In this regard, Section 4.1 of the ISDP clarifies that all (N)ADOs must comply with this International Standard, even when its requirements exceed those arising under their applicable data protection and/or privacy laws. Section 4.2 of the ISDP further specifies that, where (N)ADOs are subject to data protection and privacy laws, or other laws on the processing of personal data imposing requirements exceeding those arising under the ISDP, they must ensure that their data processing complies with such data protection and privacy or applicable laws. The EDPB welcomes these provisions, as they seem to imply that where data protection and/or privacy laws do not exist or offer a relatively lower level of protection for the rights and freedoms of the individuals concerned with regard to their personal data, these safeguards will take precedence and they would not undermine the application of data

[12] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[13] See the Annex to the Letter sent by the Chair of the EDPB to the Presidency of the Council of the EU on 9 October 2019 (Ref: OUT2019-0035), page 3.

protection and privacy laws, or other laws regulating the processing that set out a higher level of protection of personal data, such as the GDPR.

3. However, the EDPB stresses that it does not always seem easy to determine whether or not the requirements of the ISDP exceed those of applicable national law. As mentioned in its previous correspondence, the EDPB is strongly in favour of promoting the protection of privacy and personal data in the context of anti-doping activities, as reflected in the Standard. Nevertheless, the EDPB wonders whether it will be possible to apply Sections 4.1 and 4.2 of the ISDP from a strictly legal perspective, especially where the implementation of the provisions of the ISDP would lead (N)ADOs to infringe their obligations stemming from applicable laws. In the same vein, the EDPB questions the effectivity of Section 4.2 where the application of the higher safeguards provided for by data protection and privacy laws, or other laws governing the processing of personal data would expose (N)ADOs to the consequences established by Section 24.1.12 of the Code for failure to comply with the Code and/or its International Standards. In addition, allowing Member States or (N)ADOs to choose the applicable regulation may lead to inequality of treatments between athletes and other persons concerned.

4. Moreover, the EDPB notes that unfortunately the Code and the ISDP have several exceptions from the safeguards provided to protect the right to privacy and data protection that in practice allow the application of lower standards for privacy and data protection. For instance, with regard to retention periods, Sections 11.4 and 11.5 of the ISDP and its Annex A, as well as with regard to the purpose limitation principle, Section 6.2 of the ISDP. The EDPB recommends to limit any possible deviations from the safeguards provided for by the ISDP to the extent necessary for specific and important objectives of public interest and to frame the scope of the exceptions in stricter terms. That way, (N)ADOs can rely on the exception only when they are proportionate to the aim pursued with respect to the essence of the rights to privacy and data protection and implement suitable and specific measures to safeguard the fundamental rights and the interests of the concerned persons.

2. Clarify the roles and responsibilities of data controller and processor

5. In the same vein as the EDPB noted in its Letter of 2019[14], and in light of the Second Opinion 4/2009 of the Art. 29 WP[15], the latest version of the Code and the Standards still lack references to the roles of data controller and data processor for specific processing activities. This issue is crucial because it affects how data protection responsibilities are assigned and managed, which is particularly relevant for non-EEA entities acting as data controllers within the EEA or those collecting data from individuals who are in the EEA[16].

[14] Letter sent by the Chair of the EDPB to the Presidency of the Council of the EU on 9 October 2019 (Ref: OUT2019-0035).

[15] Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations, adopted on 6 April 2009, WP 162.

[16] As per Article 3 of the GDPR (Territorial Scope), the Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the monitoring of their behaviour as far as their behaviour takes place within the Union.

6. The EDPB understands that the records of data processing for anti-doping activities within the Code's scope (N)ADOs must maintain, according to Section 5.2 of the ISDP, could be seen as a simplified version of the records of processing activities required under Article 30 of the GDPR. However, unlike Article 30(1)(b) of the GDPR, which requires specific documentation of purposes, the ISDP only requires documentation of the *"general"* purpose of processing, which then may be not sufficiently defined. **Thus, the EDPB recommends amending Section 5.2 of the ISDP accordingly.**

7. In the comment on Section 5.2(a), the ISDP stipulates that (N)ADOs are required to maintain a record of their processing activities. Furthermore, with respect to the ADAMS database administered by WADA, WADA shall maintain and provide access to documentation concerning data processing within the ADAMS database. However, the specific roles of (N)ADOs and WADA (i.e. controller, joint controllers, processor) in relation to the database and for each processing activity therein are not clearly defined.

8. **In light of the above, the EDPB recommends that the ISDP includes a requirement for organisations within the scope of the Code to identify their role, corresponding to that of the GDPR for each processing activity, in particular concerning the ADAMS database, specifying whether they are a controller, processor, or joint controller.**

9. Moreover, the records to be maintained by (N)ADOs under Section of the 5.2 ISDP do not currently include all data flows, such as potential international transfers. To comply with Article 30(1)(a), (e), and (f) of the GDPR, the records must include the corresponding retention periods, the controller for each processing activity, and information on any potential international transfers. **The EDPB recommends amending the records under Section 5.2 ISDP accordingly, and ensuring that the records encompass all data processing activities including those that may be foreseen in other WADA Standards.**

3. Identify appropriate legal bases

10. Furthermore, the EDPB has concerns as to whether some of the legal grounds for processing activities envisaged by Section 7.0 of the ISDP can be considered valid.

11. First, the EDPB underlines that consent as described in Section 7.2 of the ISDP cannot be considered as “freely given” in line with Articles 6(1)(a), 7 and 9(2)(a) of the GDPR and therefore, questions whether consent can be used as a valid legal ground by (N)ADOs for the processing of personal data. Consent can only be an appropriate legal basis if a data subject is provided with a genuine choice with regard to accepting or declining the terms offered, without detriment. The EDPB notes that under section 7.2(a) of the ISDP negative consequences may arise for individuals from their refusal to consent to the processing of their personal data, which does not align with the requirements for consent in the GDPR. Furthermore, the EDPB notes that by simply informing individuals of such negative consequences as suggested in Section 7.2(a) of the ISDP, does not render the consent valid.

12. In this regard, the EDPB stresses that consent must meet further requirements than those mentioned in the ISDP, including ensuring that data subjects are able to withdraw their consent in a manner which is as easy as granting it. **Therefore, the EDPB recommends that the Code and the ISDP should exclude the use of consent as a legal ground, unless it satisfies the requirements set out in Article 7 of the GDPR.**

13. Secondly, the EDPB questions the need to use vital interest as a valid legal basis, as outlined in Section 7.1 of the ISDP. The concept of vital interest is interpreted in a very restrictive manner and has a very limited scope under the GDPR. It can only be used for limited and specific cases, such as protecting someone's life in an emergency. The EDPB is therefore not convinced that the objectives pursued by the Code would fall under this legal basis. It may be the case that personal data may be processed for vital interest in very specific circumstances. However, this does not correspond with or align with the EDPB's reading of section 7.1 of the ISDP, which is far broader in scope and applies to e.g. to data processing foreseen in the International Standard for Results Management (hereinafter 'ISRM'), where medical findings are to be announced to the (N)ADO and athlete.

14. **Therefore, the EDPB recommends revising section 7.1 of the ISDP in its entirety, and in general whether the use of 'vital interest' can be used and considered to be a valid legal ground throughout the Code. Another solution is to restrict the use of vital interest as a legal ground as prescribed by Recital 46 of the GDPR (i.e. only where the processing cannot be manifestly based on another legal basis).**

15. **In light of the above, the EDPB considers that where the legal grounds of consent and vital interest do not meet the requirements of the GDPR, (N)ADOs should rely on alternative legal bases, such as those listed in Section 7.1a of the ISDP.**

4. Ensure data is processed for specified, explicit and legitimate purposes

16. The EDPB finds that the defined list of anti-doping activities in Sections 3.1, 4.1 and 6.1 of the ISDP covers a broad range of activities from testing to education as purposes for processing personal data.

17. Concerning section 6.1 of the ISDP has been changed in its entirety, limiting the processing of personal data to one purpose (i.e., the fight against doping), and stating that only "relevant" and "proportionate" personal data may be processed. The comment on this section reads that (N)ADOs must examine the Code and its Standards to determine what personal data is required. It also adds that in many cases, the personal data to be collected by (N)ADOs will be identified by the ISDP.
18. In order to strengthen the data protection measures in the ISDP, the EDPB recommends to explicitly include additional principles: first, for the (N)ADO to process personal data in accordance with a specific, explicit and legitimate purpose and secondly, to ensure that personal data to be processed is adequate, relevant and limited to what is necessary in relation to the purpose. **The EDPB recommends a solution to the above by requiring**

(N)ADOs to implement technical and organisational measures to ensure data minimisation.

19. Although the EDPB appreciates the articulation of the principle of purpose limitation mentioned above, it is noted that Section 6.2 of the ISDP appears to broaden the scope of processing activities beyond those described in the Code to, "to engage effectively in the fight against doping", which may be problematic in upholding the data protection standards aimed by the Code. **The EDPB recommends revising Section 6(2) of the ISDP to limit the conditions for processing outside the circumstances outlined by the Code only to that which is necessary to achieve a specific, explicit and legitimate purpose. In addition, the EDPB recommends requiring in Section 6.2 of the ISDP to carry out data protection risk assessments, as well as the implementation of mitigating measures as strict requirements to be met prior to the processing (i.e. "shall", rather than "may").**

20. According to Section 6.3 of the Code, biological samples, analytical data and doping control information can be further used for anti-doping research purposes as well as for quality assurance, quality improvement, method improvement and development or to establish reference populations. However, while the further use of samples for anti-doping research purposes requires the athlete's consent, this is not prescribed for further using samples analytical data and doping control information for quality assurance and the other related purposes . According to the definition provided for by the Code[17], it seems that anti-doping research encompasses different types of researches, including "scientific investigation". In this regard, the EDPB reminds that only further processing for "scientific research" purposes[18] is presumed to be compatible with the initial purpose of data collection and where that is the case - under certain conditions and provided that appropriate safeguards for the rights and freedoms of the persons concerned are in place, as required by Article 89(1) of the GDPR – (N)ADOs may be able to rely on the legal basis of the original processing [19].

21. Therefore, the EDPB stresses that analytical data or any other personal data can be further processed for anti-doping (non-scientific) research, quality assurance or other related compatible[20] purposes only if such further processing is based on a valid legal ground according to the GDPR[21]. Moreover, since the processing of health data will be prevalent in this context, ((N)ADOs) must still assess which exception to the prohibition to process special categories of personal data, pursuant to Article 9(2) of the GDPR, may be applicable.

---

[17] See Sections 19.1 and 19.2 of the Code.

[18] With regard to the notion of scientific research purposes, the EDPB held that "*'scientific research'* […] *means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice*." See the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020, paragraph 153.

[19] See the EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), adopted on 23 January 2019, paragraph 31.

[20] Under Article 6(4) of the GDPR.

[21] Recital 50 of the GDPR.

22. Even though according to Section 6.3 of the Code, samples, analytical data and doping control information can be further used for anti-doping research purposes as well as for quality assurance and other related purposes, Article 6.2 of the Code lists a broad range of other purposes for which samples, analytical data and doping control information "shall be analysed", some of which are not well defined. The EDPB recommends identifying more precisely these purposes, particularly those concerning "DNA or genomic profiling" as well as those included in the expression "any other legitimate anti-doping purpose". Moreover, the EDPB stresses that genetic data contained in biological samples are particularly sensitive taking into account not only the inherent risk of identification, of the athletes who provided the sample, even if their identity is removed, given the unique nature of certain genetic profiles[22], but also considering that they contain information, including health data, on their biological relatives.

23. Moreover, Section 6.3 of the Code specifies that samples and related analytical data or doping control information to be further used shall first be processed in a manner to which prevents data from being traced back to a particular athlete. However, this does not entail that samples and other personal data used for either research or quality assurance purposes must be effectively pseudonymised or made anonymous, as is assumed by the document made available by WADA, summarising the major changes to the Code[23]. On the contrary, as per the International Standard for Laboratories (hereinafter 'ISL'), it is only required to remove or irreversibly alter direct identifiers from samples and analytical data before their further use for the said purposes. In addition, it is not clear if the same applies to anti-doping control information, as they are not mentioned at all by the ISL[24]. **The EDPB recommends revising Section 6.3 of the Code to the effect that the re-use of samples, analytical or other personal data (including health data or other categories of data related to anti-doping control) for research purposes (or other compatible purposes) must be subject to the implementation of appropriate safeguards for the rights and freedoms of the persons concerned in order to, in particular, ensure respect for the principle of data minimisation. In addition, the EDPB encourages to specify that those measures should include pseudonymisation or anonymisation provided that those purposes can be fulfilled in those manners[25].**

24. Furthermore, the EDPB welcomes the introduction in the Code of Sections 19.4 and 19.6 that respectively prescribe the compliance with ethical standards and practices and prevent that personal data may be further used against the person who provided the sample.

25. The International Standard for Intelligence and Investigations (hereinafter 'ISII') mentions under Section 4.3.2 that (N)ADOs shall use raw information and/or anti-doping

[22] As underlined by the Art. 29 WP in the Opinion 05/2014 on Anonymisation Technique, adopted on 10 April 2014, WP216: "*It has already been shown in the literature that the combination of publically available genetic resources (e.g. genealogy registers, obituary, results of search engine queries) and the metadata about DNA donors (time of donation, age, place of residence) can reveal the identity of certain individuals even if that DNA was donated "anonymously"".*

[23] Ibid.

[24] See article 5.3.8.2 of the ISL.

[25] See article 6.4(e) and 89 of the GDPR.

intelligence to inform and guide its anti-doping activities. The EDPB considers that the definitions of raw information and anti-doping intelligence are too broadly defined. Taking the highly sensitive nature of any investigation and inspections on the use of doping into account, the EDPB is of the opinion that any processing of personal data for the purposes covered by the ISII is likely to result in high risks to the individuals concerned. **Therefore, the EDPB recommends amending the ISII to clearly limit the scope of, and the information that can be used in, processing activities for investigation and intelligence purposes.**

26. In addition to what has been held above, the EDPB recommends that the data processing purposes of investigation should be specified clearly. Section 5.2 of the ISII leaves broad room for other, non-specified purposes to process personal data by using wording such as *"includes, but is not limited to*". Any further processing of personal data for other purposes should only be allowed subject to the conditions for establishing the compatibility of purposes such as specified under Article 6(4) of the GDPR and in accordance with a valid legal basis[26]. **Accordingly, the EDPB recommends the ISII to be amended and aligned with Section 6.2 of the ISDP. A similar observation is to be referred to Section 5.3.5 of the ISII, where the encouragement to (N)ADOs to "*make use of all investigative resources and powers available*" pertains to personal data. In the EDPB's view this should apply only insofar as processing is necessary, and only for the purposes pursued in the ISII.**

5. Require additional safeguards when sharing Personal Data with third parties

27. Under sections 9.1 and 9.2, the ISDP imposes certain requirements for the sharing of personal data by (N)ADOs with other *"persons",* that according to the Standard are defined as natural persons, organisations or other entities. The EDPB considers this definition too broad and recommends to further specify it. **The EDPB also recommends specifying in these Sections in which circumstances, for which specific purposes, and under which conditions the sharing of personal information to other 'persons' is allowed.**

28. **In addition, to strengthen the level of protection of personal data, the EDPB recommends that the ISDP requires additional measures concerning the sharing of such data to ensure that:**
    - **recipients do not process the personal data outside limited specific, explicit and legitimate anti-doping purposes which justify the sharing and that must be identified by the Code. In this regard, the EDPB recommends to clarify the term "*compulsory legal process*" that is referred to in Section 9.1.c of the ISDP as a possible circumstance allowing that sharing;**
    - **(N)ADOs only share the personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which such data need to be shared;**

[26] Recital 50 of the GDPR.

- **the personal data are kept by recipients for no longer than is necessary for the purposes for which they are shared and deleted or rendered anonymous (in such a manner that the data subject is not or no longer identifiable) when such data is no longer necessary;**
- **the recipients to whom personal data is shared have appropriate security measures in place that ensure the integrity and confidentiality of the received personal data.**

29. Section 9.3 of the ISDP includes requirements to ensure that personal data will only be shared in a responsible manner with third party agents including the implementation of technical and organisational security measures. **The EDPB recommends incorporating an additional requirement to this section providing that where and if data processing activities are carried by third party agents acting as data processors on behalf (N)ADOs they must be based on contract or legal act in line with Article 28 of the GDPR. Under the terms of the this contract or legal act, third party agents must act under documented instructions[27] of and provide assistance to (N)ADOs so that they can ensure compliance with the ISDP and the GDPR, including but not limited to guaranteeing the security of personal data, responding to requests for exercising the data subject rights', as well as obligations relating to personal data breaches.**

30. When these processing activities, carried out by third party agents, entail the international transfer of personal data, equivalent safeguards to those provided by Chapter V of the GDPR should be put in place[28].

31. With regard to transfers made from EEA-based (N)ADOs to the ADAMS database, the European Commission renewed, in January 2024, Canada's adequacy status under the GDPR, confirming that the level of protection ensured by the PIPEDA is adequate. Thus, the EDPB is of the view that transfers taking place on this basis continue to be valid. However, if transfers were to be undertaken directly between (N)ADOs and were not covered by the adequacy decision of Canada, those categories of transfers should be described in the Code and the exporting (N)ADO should ensure the respect of Chapter V of the GDPR and applicable EDPB guidance[29].

32. When it comes to the sharing of anti-doping intelligence in accordance with Section 4.2 of the ISII, such an obligation to share personal data should be based upon an appropriate legal ground in line with Article 6 of the GDPR. When such activity involves an international transfer of personal data, the EDPB recommends to ensure that the GDPR rules set out in its Chapter V of the GDPR should be adhered to, to ensure that the level

[27] Please note that the reference made to *"contractual controls that can include, as appropriate"* in the comments to Section 9.3.b of the ISDP is not in line with the GDPR.

[28] See for instance in this regard the standard contractual clauses under the GDPR issued by the European Commission for data transfers from controllers or processors in the EU/EEA to controllers or processors established outside the EU/EEA (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council).

[29] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted on 18 June 2021; See also Judgement of the Court of Justice of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559 (Schrems II).

of protection of natural persons guaranteed by it is not undermined[30]. **Considering the scope of the Standards and international element involved in the activities of organised sports into account, the EDPB highly recommends to lay down in the ISII specific and clearly defined rules on investigation and inspection, including for the sharing and international transfer of personal data.**

6. Public Disclosure of Anti-Doping Violations

33. Concerning mandatory public disclosure of anti-doping rule violations, the EDPB firstly welcomes the amendments proposed to Section 14.3.2 of the Code which clarify that the mandatory public disclosure only concerns final decisions (regarding anti-doping rule violations by professional athletes or other persons committing the violation)[31]. As for the exceptions to the generic principle envisaged by Section 14.3.4 of the Code, requiring the athlete's or other concerned person's consent for publishing, after a hearing or appeal, determinations establishing that they have not committed an anti-doping rule violation, or they bear no fault or negligence, the EDPB reiterates that consent to process personal data must meet the requirements of the GDPR, in particular that it is freely given.

34. Moreover, with regard to the newly introduced provision which entails that (N)ADOs can do without the athlete's or the other person's consent, if their identity is already public or consequences have already been imposed, the EDPB questions whether this exception takes adequately into account that the publication may be in the interest of the athlete or other person concerned.

35. The EDPB welcomes Section 14.3.7 of the Code which establishes that the mandatory public disclosure shall not be required where the athlete or other person who has been found to have committed an anti-doping rule violation is a minor, a protected person, or a recreational athlete and that any discretionary public disclosure shall be proportionate to the facts and circumstances of the case where such persons are involved.

36. However, to ensure that a right balance is struck between the reasons that justify a certain degree of transparency regarding anti-doping rule violations and the need to safeguard the fundamental rights and interests of the person concerned, the EDPB recommends specifying that the elements to be taken into account in this regard are, among others, the severity of the anti-doping rule violation, the number of violations, whether the case has already received media attention, the particular situation of the concerned data subject, and whether the sanction has consequences for the results of competitions and ranking of athletes. The same criteria should guide the (N)ADOs' decisions in the remaining cases of discretionary public disclosure regulated by Section 14.3.1 of the Code.

[30] Chapter V, art 44 – 50 of the GDPR.

[31] In this regard, a request for a preliminary ruling is pending in front of the CJEU: NADA Austria and Others, case C-474/24.

7. Define specific retention periods, limited to what is necessary to achieve each Purpose

37. The EDPB welcomes that the ISDP frames maximum retention periods for (N)ADOs. As per the principle of storage limitation under Article 5(1)(e) of the GDPR, the retention of data must be closely linked to the specific and legitimate purpose(s) of processing. However, Annex A of the ISDP does not clearly link the defined retention period for each dataset to a specific, explicit and legitimate processing purpose. Therefore, the EDPB recommends that the Modules listed in annex A indicate the corresponding specific, explicit and legitimate purpose(s) of processing for each dataset concerned.

38. Contrary to the wording of Section 11.2 of the ISDP, (N)ADOs should always define a retention period for the processing of personal data according to Article 5(1)(e) of the GDPR. **Therefore, the EDPB recommends deleting the wording "*where possible*" in this section.**

39. The EDPB welcomes that Section 11.3 of the ISDP ensures the deletion, destruction or anonymisation of personal data once it is no longer required. As the data concerned in the field of anti-doping is mostly sensitive, mitigating measures must ensure the respect of fundamental rights and freedoms of the individual. The explanation to the wording of Section 11.3, sentence 3 of the ISDP, requires stronger reasons for keeping sensitive data for which no retention time has been set in Annex A of the ISDP[32], but those are not defined in the section itself. **The EDPB recommends to clearly set out rules, legal grounds and mitigating measures for sensitive data to be kept where no retention time has been set in Annex A of the ISDP .**

40. The EDPB takes note that Sections 11.5 and 11.6 of the ISDP allow for data storage beyond the defined retention periods. The exceptional circumstances in Section 11.5.c of the ISDP refer to a "*pending or reasonably anticipated anti-doping rule violations, investigations, or other legal proceedings*". The EDPB notes that the term referring to reasonable anticipation of anti-doping rule violations is unclear and recommends to clarify this term. These exceptional cases in Section 11.5.a of the ISDP include an applicable law that allows for longer storage than Annex A of the ISDP. In light of the understanding that the Code should be a common minimum standard for the processing of personal data for anti-doping purposes, no other laws envisaging longer storage should be applied.

41. According to Annex A to the ISDP, the defined retention periods shall not prevent the (N)ADO from keeping records "*stripped of Personal Information*" for longer periods. **The EDPB recommends to clearly indicate that this statement refers to anonymised data.**. With reference to Important Note III, the EDPB recommends that for the removal of incomplete data for data quality purposes to align with the principles of data accuracy, and integrity under Article 5(1)(d), and (f) of the GDPR, the word "should" to be replaced with "must".

[32] See Section 11.2 of the ISDP.

42. As a general remark, the EDPB considers the retention period of 10 years to be very long, taken into account that personal data may include geolocations and even data of minors. The EDPB recommends providing further reasoning on the overall 10 year maximum retention period that balances appropriately the interests of the data subjects with those of (N)ADOs.

43. The data in Module 2 include addresses for regular activities, overnight accommodations and contact information of Athletes. Since this may be qualified as profiling, the retention period should be much shorter than 10 years. The retention of such data should be limited to where the personal data included in the whereabouts are no longer relevant. In addition, Section 4.10.13.1 of the IST no longer requires athletes to submit their 'regular activities', but instead only their training locations and relevant timeframes. The EDPB welcomes this amendment but recommends that change to be implemented in Annex A of the ISDP.

44. The Module 3 for data of therapeutic use exemptions includes health data. Whereas the retention period of 12 months after expiry for additional medical data seems reasonable, the TUE certificates and rejections forms are kept for 10 years, as they "*can be relevant for re-testing or other investigations*". For rejection forms in particular, the EDPB suggests that WADA revise the retention period in line with the specified purpose and limit it to what is strictly necessary.

45. In Module 7 of Annex A of the ISDP, a retention period of 10 years following closure is defined for investigation records. The EPDB questions the proportionality of keeping such records for 10 years, especially considering the fact that not every investigation leads to a finding of a violation of anti-doping rules. In such circumstances, a standard retention term of 10 years is likely to be disproportionate.

46. According to Module 8 in Annex A of the ISDP, data on courses and dates of educational are retained "*until all other associated record are deleted*" or the person is no longer active. This definition of a retention period is too vague and should be specified in greater detail. This is also to ensure that the persons concerned can understand the timeline of the data processing.
47. In light of the above, the EDPB recommends to revise the retention periods, particularly considering the necessity of each data item with respect to the purpose justifying each processing operation.

8. Provide further directions to enhance the implementation of the principle of Data Protection by Design by organisations

48. The EDPB welcomes the implementation of the privacy by design concept to the ISDP and appreciates that it explicitly mentions additional security controls and data minimisation measures as examples. However, the elements listed in section 5.1 of the ISDP do not fully cover the requirements of Article 25(1) of the GDPR. The concept of privacy by design as envisaged under the GDPR requires (N)ADOs, acting as controllers, to incorporate data protection measures into the design of their systems and processes. The

EDPB notes that the ISDP does not include requirements to implement this concept. **Therefore, the EDPB recommends including in the ISDP specific requirements for (N)ADOs to implement technical and organisational measures to support the concept of privacy-by-design. This recommendation could also apply to data processing activities outlined in other Standards, such as the sharing of laboratory results via ADAMS as described in the ISRM.**

9. Processing of Special Categories of Personal Data

49. The EDPB notes that the processing of personal data envisaged by the Code and ISDP entails significant processing of what is termed "*sensitive personal information*". The EDPB notes that the definition of sensitive personal information in the ISDP is somewhat similar to that of special categories of personal data under Article 9 of the GDPR. The EDPB recommends that the definition of sensitive personal data be amended to correspond to Article 9 of the GDPR. The EDPB also reiterates that processing of personal data relating to criminal convictions and offences should be carried out only under strict conditions such as required by Article 10 of the GDPR.

50. The EDPB welcomes the requirement at Section 5.3 of the ISDP that sensitive personal information must be processed in accordance with specific safeguards or procedures under applicable privacy and data protection laws. In this regard, the EDPB notes that the processing of special categories of personal data is generally prohibited under the GDPR, unless one of the derogations pursuant to Article 9(2) of the GDPR applies[33].

51. However, the EDPB notes that the wording of Section 5.3 of the ISDP is quite general, stating that sensitive information must be processed in accordance with "*any specific safeguards or procedures*" in the ISDP and applicable privacy and data protection law without defining which precise safeguards must be put in place. The additional restrictions mentioned are not detailed in the ISDP, and Sections 10.3 or 11.3, for example, do not seem to spell out further safeguards to ensure security and limited retention of such data.

    Section 7.3 of the ISDP specifies that when sensitive personal information is processed based on consent, the explicit consent of the individual concerned shall be obtained. Noting that explicit consent in this context aligns with Article 9(2)(a) of the GDPR, the EDPB reiterates its concern that consent may not represent an appropriate legal basis for processing personal data (including special categories of personal data) under the Code and the ISDP[34].

52. **Therefore, the EDPB recommends that the ISDP is amended with reference to the sensitive nature of the data processing envisaged, and that it specifies which types of safeguards can contribute to the protection of special categories of personal data in line with Articles 9(2), 25(1) and 32 of the GDPR.**

[33] See Section 4 above.
[34] See Section 3 above.

10. Clarify the role of the Person designated as accountable for compliance with all applicable privacy and data protection laws

53. The EDPB notes the requirement in Section 4.4 of the ISDP that "*Anti-Doping Organizations shall designate a Person who is accountable for compliance with this International Standard and all applicable privacy and data protection laws. They shall ensure that the contact information of the Person so designated is made readily available to individuals in accordance with Article 8.*"

54. While the EDPB welcomes the inclusion of a requirement for the designation of a person responsible for data protection compliance within (N)ADOs, it is not clear to what extent the role of the person envisaged under Section 4.4 of the ISDP aligns with that of the data protection officer ('DPO') pursuant to Articles 38-39 of the GDPR.

55. Section 4.4 of the ISDP states that the designated person shall be "*accountable for compliance with* […] *all applicable privacy and data protection laws"*. However, the principle of accountability pursuant to Article 5(2) of the GDPR, makes it clear that the controller (the (N)ADO itself in this instance) shall be responsible for, and be able to demonstrate compliance. DPOs designated in accordance with the GDPR should be in a position to perform their duties and tasks in an independent manner, and without any instruction from the controller regarding the exercise of those tasks. In this regard, DPOs cannot be held accountable for compliance with the GDPR in the same manner as controllers, as the designated person can under Section 4.4 of the ISDP. Finally, the EDPB notes that Section 4.4 is not clear as to whom the designated person shall be accountable.

56. The EDPB notes, and welcomes, that the requirement under Section 4.4 of the ISDP to make the contact information of the designated person available to individuals aligns with that of Article 37(7) of the GDPR, concerning the publication of the contact details of the DPO.

57. Notwithstanding Section 4.4 of the ISDP, (N)ADOs subject to the GDPR must be cognisant of their obligation to determine whether designation of a DPO is mandatory according to the criteria set out in Article 38(1) of the GDPR. While the latter mandates the designation of a DPO in specific circumstances within its scope, (N)ADOs not subject to the GDPR may wish to appoint an equivalent person to ensure adherence to applicable data protection laws, regulations, and the requirements of the ISDP. This responsible person/team should have sufficient authority, resources, and expertise to effectively oversee privacy practices, manage data protection risks, and serve as a primary point of contact for privacy-related matters. Their responsibilities include monitoring compliance, managing privacy programs, conducting assessments, and coordinating with relevant stakeholders and supervisory authorities where applicable.

58. **Therefore, the EDPB recommends that it is clarified whether the role of the designated person under Section 4.4 of the ISDP is intended to be equivalent to that of the DPO under GDPR, and if so, to align the roles in terms of their designation, position, and tasks. Without such clarification, the EDPB considers that Section 4.4 may give rise to a**

risk that (N)ADOs subject to GDPR will not fulfil their obligations as data controllers under Articles 37-39 of the GDPR.

11. Ensure effectiveness of Data Subject Rights

59. The EDPB welcomes the provisions of Section 8 of the ISDP relating to the provision of information to individuals. The EDPB recommends that the scope of information to be provided should specifically include reference to the collection of raw information and anti-doping intelligence as set out in the ISII.

60. The EDPB welcomes the provisions of Section 12 of the ISDP whereby individuals have the right to obtain from (N)ADOs access to their personal data and information on how they are processed, and the implementation of requirements which (N)ADOs must follow in order to allow the exercise of such data protection rights. However, the EDPB also notices that the substantive requirements under Sections 12.1.c, 12.2, 12.3 and 12.4 of the ISDP are inconsistent with the data subject rights under the GDPR.

61. In particular, the ISSPI in its Section 12.1.c provides an exception to the right to obtain a copy of personal data when this "*plainly conflicts with the integrity of the anti-doping system or an Anti-Doping Organization's ability to plan or conduct No Advance Notice Testing or to investigate and establish anti-doping rule violations or other legal claims*." As highlighted in its previous correspondence[35], the EDPB considers that the derogation is formulated in particularly vague terms and it does not, on the face of it, appear to be in conformity with the GDPR.

62. In addition, Section 12.2 of the ISDP states that (N)ADOs have to respond to a request for access by a data subject, except if doing so imposes a disproportionate burden on (N)ADOs. Under Section 12.3, it is established that when (N)ADOs refuses to allow individuals access to their personal data, the individual must be informed about the reasons for refusing the request "*as soon as practicable*". The EDPB notices a similar approach to Section 12.4 of the ISDP whereby personal data may not be rectified and amended if it proves to be impossible or a disproportionate effort. In light of the above, as the interests of both individuals and those of (N)ADOs do not seem to be appropriately balanced, the EDPB questions whether the rights of individuals with regard to their personal data are effectively guaranteed by the ISDP.

63. In this respect, the EDPB reiterates that any restrictions to data protection rights is only allowed if it conforms to the conditions se out of Article 23 of the GDPR which authorises Member States to adopt legislative measures aiming to restrict the scope of such rights insofar as this restriction respects the essence of the fundamental rights and freedoms of individuals and is a necessary and proportionate measure in a democratic society.

[35]Letter sent by the Chair of the EDPB to the Presidency of the Council of the EU on 9 October 2019 (Ref: OUT2019-0035), page 8.

64. **Therefore, the EDPB recommends revising Section 12 of the ISDP to mirror Articles 12-15 of the GDPR and any respective EDPB Guidelines as well as the conditions set out in Article 23 of the GDPR with regard to any possible restrictions to data subjects' rights**

65. **Lastly, the EDPB restates that the Code should contain a right of remedy and a right of compensation for the damage suffered by individuals as a result of a processing operation incompatible with the ISPD[36].**

For the European Data Protection Board

The Chair

(Anu Talus)

[36] Ibid.