

Strasbourg, 5 June 2020

T-MC(2020)55

Convention on the Manipulation of Sports Competitions (Macolin Convention)

Group of Copenhagen

Macolin Convention Data Protection Principles (draft v. 2)¹

Executive Summary

The Data Protection Standard (the “Standard”) comprises a set of high level requirements, grounded in international data protection frameworks which is Convention 108 as amended by the Protocol CETS 223 (modernised Convention 108) for the Council of Europe, that National Platforms are expected to comply with when processing personal data pursuant to the Macolin Convention on the Manipulation of Sports Competitions (the “Macolin Convention”).

Recognizing that National Platforms, and their individual members, commonly process (i.e collect, use, share, etc.) with other parties personal data relating to, amongst others, athletes, athlete support personnel, event organizers, and members of the public in connection with their efforts to prevent, investigate, prosecute and sanction those engaged in the manipulation of sport, the Macolin Convention requires due regard be given to the protection of privacy and personal data of individuals. This includes, in particular, “the principles of lawfulness, purpose limitation, necessity and proportionality, high level of data quality, transparency, accountability and also to data security and the rights of data subjects as well as an effective, independent oversight”.

The Standard is to serve National Platforms in their endeavor of establishing a baseline set of data protection requirements which guarantee an appropriate level of protection for individuals while facilitating the free flow of data among them, to which National Platforms are expected to adhere. These requirements, which take the form of high-level principles, serve as a floor, and National Platforms are free to exceed them should they choose to do so. That said, they take into account the level of protection established by the modernised Convention 108 in line with art 14 of the Macolin Convention and art 122 of its Explanatory Report, and thus set a higher bar than exists in many countries that are not Party.

While conceding the lawful use of exceptions in appropriate cases, the Standard obliges National Platforms to comply with the following core principles when processing personal data, understood broadly to include the collection, use, storage, transfer, subsequent use and disclosure of data:

- fair and transparent processing: meaning ensure that the processing that takes place reflects a fair balance between all interested concerned, is sufficiently transparent and made known to the relevant individuals;
- purpose limitation and legal basis: meaning ensure processing is only for specified, explicit and legitimate purposes, and only process data where there is a valid legal basis to do so;

¹ Drafted with the assistance of Mr Daniel Cooper, Consultant for the Committee of Convention 108 on Data Protection

- proportionality, integrity and retention: meaning only process data where it is necessary and proportionate to the legitimate aim pursued, adopt measures to maintain the a high quality of the data and delete data as soon as possible;
- rights of individuals: meaning respect rights individuals have in relation to their data, such as rights of access, correction, restriction and objection;
- disclosures and transfers: meaning protect data when disclosing or transferring data, and only do so where certain conditions are met;
- data security: meaning implement measures to protect data against accidental or unauthorized access by third parties, and notify competent authorities in the event a breach of security impacting data subject occurs;
- accountability: meaning take appropriate measures to comply with data protection obligations arising under law and keep internal records to demonstrate compliance with the Standard; and
- oversight and redress: meaning cooperate with supervisory authorities in relation to data protection matters, including the resolution of complaints by individuals.

It is expected that adherence to these basic principles will better align the practices of National Platforms with global data protection laws, and provide a basis for further, more detailed guidance to be developed by the Group of Copenhagen.

Introduction

Referring to Article 14 of the Macolin Convention on the Manipulation of Sports Competitions, the Group of Copenhagen, has decided to address questions related to data protection arising from the exchange of information within and among National Platforms.

Following from the Diagnosis Report [document T-MC(2019)53], the present document is meant to serve as a tool to help ensure *“that ongoing action against the manipulation of sports competitions comply with relevant national and international personal data protection laws and standards....”*

This Data Protection Standard (“Standard”) sets out data protection principles the undersigned National Platforms and other data controllers agree to abide by and respect when carrying out any personal data processing (including personal data sharing activities), both independently and in cooperation with other National Platforms or third parties, in furtherance of the aims of the Macolin Convention.

The Standard is to be sent to the Committee of Convention 108 for its official opinion and possible further guidance in the framework of an agreement between the GoC and the Committee of Convention 108 in assisting Parties to the Macolin Convention and other interested stakeholder to comply with their legal obligations on the basis of the modernised Convention 108.

Data Protection Standard

1. Purpose and Objective

The purpose of this Standard is to better ensure that National Platforms, and their constituent members, collecting, sharing and processing personal data pursuant to the Macolin Convention and its Explanatory Report do so in a manner that conforms with commonly applied data protection rules and principles.

The following principles are based on Convention 108 as modernised by the amending Protocol CETS 223 (Modernised Convention 108), as the international standard in the field of the protection of personal data and provide a set of common core standards shared by Parties to the Macolin Convention and are without prejudice to any data protection requirements that exceed or go beyond the present principles under applicable national laws.

2. Definitions

For the purposes of this Standard:

- a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);
- b. “data processing” means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;
- c. Where automated processing is not used, “data processing” means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;
- d. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;
- e. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
- f. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

3. Fairness and Transparency

The National Platforms will process personal data fairly and transparently. This includes, in particular informing data subjects about the purposes of any data processing that occurs, the identity of data controller(s) (or the equivalent concept under applicable data protection laws), the legal basis and the purposes of the intended processing, the categories of personal data collected, to whom it will be disclosed, the rights of the data subjects and the means to exercise them, how to contact the National Platform with any inquiries or complaints, how to obtain redress and the possibilities and means offered for limiting use and disclosure of personal data as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

4. Purpose Limitation and Legal Basis

The National Platforms will process personal data only for specified, explicit and legitimate purposes, and will not use it for purposes incompatible with the purposes for which it was originally collected. For the avoidance of doubt, processing for statistical or research purposes will be deemed compatible with any original processing that takes place subject to appropriate safeguards.

The National Platforms will only process personal data to the extent that it has a valid legal basis to do so. Data processing shall be carried out (including, but not limited) to comply with a legal obligation, fulfil a contractual obligation owed to the data subject, pursue a legitimate interest of the data controller or of a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject), or with the free, specific, informed and unambiguous consent of the data subject.

In addition, the National Platforms will only process sensitive personal data², as defined under applicable laws, in line with article 6 of the modernised Convention 108, when it is provided for by law, and where appropriate safeguards and measures complementing these principles (for instance, the explicit consent of the individual concerned) are in place, that are proportionate to the risk presented by the processing and that prevent or minimise the privacy risks to individuals, especially the risk of discrimination.

5. Proportionality, Integrity and Retention

The National Platforms will limit their processing of personal data to what is necessary and proportionate given the purposes for which they process data and will use all reasonable means to keep personal data accurate, complete, up-to-date and reliable for its intended use.

² Special categories of data (sensitive data) are defined in article 6 of the modernised Convention 108 as: genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

The National Platforms will take all reasonable steps to ensure that any incorrect or inaccurate personal data is erased or rectified without delay. Personal data must be kept for no longer than is necessary given the purpose or purposes for which it is processed.

6. Rights of Individuals

The National Platforms will ensure the processing of requests that data subjects make in relation to their rights, such as rights relating to access, correction, restriction or objection as enshrined in article 9 of the modernised Convention 108. The National Platforms will only engage in solely automated decision-making involving personal data that may have legal or equivalent effects on the individual where provided for by applicable laws and will allow individuals to request a human intervention when there is a decision made by the National Platforms that significantly affects him/her without having his/her views taken into consideration.

The National Platforms will respond to requests aiming at obtaining knowledge of the reasoning underlying data processing where the results of such processing are applied to the data subject.

7. Disclosures of Personal Information between members of the National Platform

National Platform members will only disclose Personal data to other members of the same National Platform where the disclosure serves the purposes of the Macolin Convention to eliminate sports manipulation and is in accordance with applicable data protection laws and this Standard.

The National Platform members will only disclose Personal data to other stakeholders, outside the National Platform, for a legitimate purpose, on a case-by-case basis, and only if there are lawful grounds for doing so, such as where required by law or compulsory legal process (including disclosures to law enforcement, tax, immigration or other authorities in connection with the performance of their statutory functions), to protect the interests of the National Platform, or with the free, specific, informed and unambiguous consent of the individual concerned. The minimum amount of Personal data shall be shared given the purposes to be served by the disclosure.

The use of cooperation agreements, memoranda of understanding and similar safeguards are encouraged and shall be used to ensure that an appropriate level of protection of personal data is guaranteed to the greatest extent possible, and the National Platforms shall refrain from disclosing personal data where they reasonably believe the recipient cannot or will not comply with these Principles.

8. International Transfers

The National Platforms in a state that is party to Modernised Convention 108 will transfer personal data to another National Platforms or third parties residing in another state that is also party to Convention 108 according to provisions laid down in it, notably in its article 14.

The National Platforms will only transfer or disclose personal data internationally, whether to other National Platforms or third parties, in accordance with applicable law and where an appropriate level of protection based on the provisions of the modernised Convention 108 is ensured. An appropriate level of protection can also be guaranteed by the law of the receiving state or by ad hoc or approved safeguards provided by legally binding and enforceable instruments.

Personal data can also be transferred in specific cases where the data subject has given free, specific, informed and explicit consent, including being informed of the risks arising in the absence of appropriate safeguards; or where the specific interests of the data subject require such transfer; or where there are prevailing legitimate interests, in particular where important public interests will be served by the transfer or the transfer is provided for by law and constitutes a necessary and proportionate measure in a democratic society.

9. Data Security

The National Platforms will implement appropriate administrative, technical, and physical measures to protect personal data from accidental or unauthorised access, destruction, loss, use, modification or

disclosure. These measures will take into account the state of the art, the costs of implementation and the nature of the processing, as well as the risk of harm to the individual arising from a breach of security.

In the event of a breach of security giving rise to a risk to the affected data subjects ("Data Breach"), the National Platform will notify the competent authorities and, where the relevant risk is serious, the data subjects concerned without undue delay. Each National Platform will maintain a record of Data Breaches that will be made available to competent regulatory authorities upon request.

10. Accountability

The National Platforms will take all appropriate measures to comply with applicable data protection obligations and shall keep internal records to demonstrate their compliance with this Standard, such as through internal policies and procedures as well as audit or assessment reports. These will include to showcase that the data processing was designed to prevent or minimise the risk of interference with data subjects' rights and to ensure the data minimisation principle (also in respect of the access to the collected data) and that the introduction of new processing of data in the National Platform is preceded by a prior assessment on its likely impact on data subjects' rights.

The Internal policies that constitute examples of best practices should be published where such a publication doesn't compromise the security of the National Platforms.

11. Exceptions and Restrictions

Exceptions and restrictions to the principles expressed in this Standard can only be made if provided for by law, which respects the essence of the fundamental rights and freedoms of individuals, such as freedom of expression and information, and constitutes a necessary and proportionate measure in a democratic society for the purpose of protecting national security, defence, public safety, important economic and financial interests of the state, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, or other essential objectives of general public interest.

In cases where the processing of the personal data is purely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the rights of data subjects under Point 5 and the transparency obligations under Point 3 may be limited or restricted by law provided this does not give rise to a risk of harm to the rights and fundamental freedoms of data subjects.

12. Oversight & Redress

The National Platforms will cooperate in good faith with any supervisory authority of competent jurisdiction and will inform individuals about the possibility of their lodging a complaint with any competent authority responsible for the protection of personal data or seeking judicial redress under law.