

Follow-up Committee

on Manipulation of sports competitions (T-MC)

Council of Europe Convention on the
Manipulation of Sports Competitions
(CETS n°215)

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Strasbourg, 11 October 2022

T-MC(2022)8

Follow-up Committee on the Manipulation of Sports Competitions (T-MC)

Data protection | Principles & guidance

Executive Summary

National Platforms, and their individual members, necessarily process (i.e. collect, use, share, etc.) personal data in connection with their efforts to comply with and implement the Macolin Convention on the Manipulation of Sports Competitions (the “Macolin Convention”).

The Macolin Convention requires in Article 14 that “[e]ach Party shall adopt such legislative and other measures as may be necessary to ensure that all actions against the manipulation of sports competitions comply with relevant national and international personal data protection laws and standards, particularly in the exchange of information covered by this Convention”, and that “when personal data are collected, processed and exchanged, irrespective of the nature of those exchanges, due regard is given to the principles of lawfulness, adequacy, relevance and accuracy, and also to data security and the rights of data subjects”.

In light of this, the [Data Protection Standard T-MC\(2020\)55](#) (the “Standard”), which comprises a set of high level requirements grounded in international data protection frameworks including Convention 108 as amended by the Protocol CETS 223 ([Convention 108+](#)), was drafted to assist National Platforms in complying with their data protection obligations with when processing personal data pursuant to the Macolin Convention.

Article 15 of Convention 108+ assigns to Supervisory Authorities the role of providing information to those processing personal data, about their responsibilities and obligations concerning data protection. This Data Protection Guidance (the “Guidance”) has therefore been developed to further assist Supervisory Authorities, National Platforms, their individual members and other actors assisting in the prevention, detection, investigation and prosecution of the manipulation of sport in understanding the data protection principles contained in the Standard. Additionally, it aims to provide examples of how these principles may be complied with in practice, for example how different actors might implement the principle of fair and transparent processing and the factors National Platform members must consider when implementing the principle of data security.

The following data protection principles will be covered under this Guidance:

- 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;
- proportionality, integrity and retention: meaning only process data where it is necessary and proportionate to the legitimate aim pursued, adopt measures to maintain the 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, and in relation to automated decision-making;
- 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 unauthorised access by third parties, and notify competent authorities in the event a breach of security impacting data subject occurs; and
- accountability: meaning take appropriate measures to comply with data protection obligations arising under law and keep internal records to demonstrate compliance with the Standard.

Data Protection Guidance

1. Purpose and Objective

The purpose of this Guidance is to expand upon and supplement the Standard by providing further explanation of the Standard's data protection principles with which National Platforms, and their constituent members, must comply when collecting, sharing and processing personal data pursuant to the Macolin Convention and its Explanatory Report. It also provides examples of how each principle might be implemented in practice, which National Platforms and their individual members may wish to consider as they implement each principle. This Guidance is meant to be helpful, and not prescriptive, and each National Platform member should take into account their applicable data protection and privacy laws and regulations.

2. Definitions

For the purposes of this Guidance:

- 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. "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;
- d. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
- e. "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 principle of fairness and transparency requires that National Platforms, when processing personal data, be clear, open and honest with data subjects about the "Who, What, Why, How, and Rights and Choices" regarding their data processing. This means informing data subjects about the identity of any data controller(s) participating in the processing, the categories of personal data collected, the purpose(s) for which the data is being processed, the legal basis on which the controller(s) and/or processor(s) are relying to carry out the processing, to whom the data will be disclosed, data subjects' rights and how they can be exercised, how to contact the National Platform Coordinator and relevant data protection Supervisory Authority 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 that National Platforms' processing of personal data is fair and transparent.

They must make this information available to those data subjects in an effective manner, such as through a privacy notice or in a contract. How individual members of the National Platforms choose to provide this information will depend upon several factors such as the nature of the organisation (e.g., public body or private enterprise; sports organisation, betting agency, and so forth), its relationship to the relevant data subjects whose data is being processed, and the type of documentation that would ordinarily be provided to the data subjects with whom they interact.

Guidance

A State's National Platform coordinator is a central governmental body that facilitates information sharing among individual members. A sports betting operator participates in the State's National Platform, collecting and transmitting personal data in connection with suspicious bets placed in its physical shops and its online betting platform.

Both the National Platform coordinator and the sports betting operator will need to consider how best to implement the data protection principle of fairness and transparency. The sports betting operator will need to provide information about its data processing activities to both in-person and online bettors, and likely will need to provide this information in different formats to each. In its physical stores, it may provide this information in a shorter, printed privacy policy that directs bettors to access its full privacy policy online. It may also place this information in a contract which bettors must read and agree to before they can place bets. For its online platform, the operator may rely on a privacy policy and/or make this information available to bettors when they create an online account.

As the National Platform coordinator does not directly collect information from data subjects placing bets, the most appropriate method of providing information to data subjects about its data processing activities may be in a privacy statement available on its website. Additionally, it requires individual Platform members such as the sports betting operator to direct data subjects to its privacy statement and inform individuals that their data may be shared with other members, like the coordinator. In all such cases, policies, privacy statements and other related materials should be drafted in a manner that is comprehensible and easy to understand for the intended recipient.

A football team also participates in the National Platform, and processes the personal data of all of its players and staff. The team could include the "Who, What, Why, How, and Rights and Choices" of its data processing in all player and staff contracts, and may also run informational sessions so that data subjects are made aware of this information.

4. Purpose Limitation and Legal Basis

The principle of purpose limitation places two requirements on National Platform members. The first requirement is that they must process personal data only for specified, explicit and legitimate purposes, and must not use that personal data for purposes incompatible with the purposes for which it was originally collected (however, processing for statistical or research purposes may be compatible with any original processing if the processing is subject to appropriate safeguards).

The second requirement is that members must only processing personal data to the extent that they have a valid legal basis to do so. The Standard underlines that data processing can only be carried out in certain situations, such as to comply with a legal obligation, to fulfil a contractual obligation owed to the data subject, to 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.

Where a State party to the Macolin Convention has enacted in national law a legal basis that allows for Macolin Convention-related data processing, this likely would be the appropriate legal basis for National Platforms and individual members to rely on when processing personal data. However, if a State has not enacted such a legal basis in its national law, the National Platform and its members must identify a suitable legal basis for their data processing activities.

Guidance

Purpose Limitations: A National Platform's members process large volumes of personal data in relation to several of their activities. They inform data subjects that a particular subset of that personal data is additionally processed to fight against sports competition manipulation in compliance with the Macolin Convention and/or national law. They must not use or process that subset of personal data for any other purpose which is incompatible with the previously stated purposes such as for direct marketing or advertising.

Legal Basis: The State in which the National Platform and its members are located has enacted a law that provides that data processing shall be lawful if it is done in order to prevent, detect, investigate or prosecute sports competition manipulation. They may therefore rely on this legal basis for all data processing which relates to this legally sanctioned purpose.

Another National Platform is located in a State that has not yet enacted a legal basis which specifically covers data processing done for the purpose of preventing, detecting, investigating or prosecuting sports competition manipulation. Members of this National Platform will therefore need to identify another suitable legal basis for data processing carried out in furtherance of the Macolin Convention, which complies with applicable law (e.g., public interest). It must be aware that a single legal basis may not be appropriate to cover all of its processing, and that it may need to rely on different legal bases for different processing activities.

5. Proportionality, Integrity and Retention

Proportionality requires National Platforms to limit their processing of personal data to what is necessary and proportionate given the purposes for which they process the data. Integrity requires them to use all reasonable means to keep personal data accurate, complete, up-to-date and reliable for its intended use, and to take all reasonable steps to ensure that any incorrect or inaccurate data is erased or rectified without delay. Finally, retention requires National Platforms to only keep personal data for as long as, and no longer than, is necessary given the purpose or purposes for which it is processed, and to maintain data retention policies that are appropriate given the purpose and legal basis of their processing and that comply with all relevant legal obligations.

Guidance

Proportionality: A sports betting operator processes the personal data of all of its customers when they place bets on its online platform. Its platform has the ability to collect and send up to 30 categories of personal data when a bet is placed, but the operator determines that only 10 of these categories of data are necessary and proportionate for it to comply with its obligations as a member of the National Platform. The sports betting operator must only process those 10 categories of personal data insofar as the processing is Macolin Convention-related processing.

Integrity: A National Platform member, a government agency, notices that the personal data which it receives from the national football association is incomplete, and is missing key information that it needs to accurately identify instances of sports competition manipulation through suspicious betting activity. The member must use all reasonable means, such as notifying the football association of the issue, to ensure that the missing data is collected. The football association must also ensure that, for example, it keeps up-to-date records of players and staff.

Retention: The member must additionally take all reasonable steps to ensure that any incorrect data received from the football association is either erased or corrected without delay, and must only keep the personal data it receives for as long as is necessary to prevent sports competition manipulation being carried out by those data subjects, and this might extend through the period of time that it required to investigate the alleged manipulation and, where appropriate, engage in legal or other proceedings. If the National Platform member no longer needs some of the personal data it has collected or, where relevant, any related criminal case is closed and all means of appeal have been exhausted, it must delete that data without delay. The member should also ensure that it has considered the aims of the Macolin Convention and the legal basis for its Macolin Convention-related processing when determining how short or long it retains the personal data, and that this retention period complies with applicable law.

6. Rights of Individuals

This principle obliges National Platform members to respect data subjects' rights in relation to their personal data, including rights relating to access, correction, restriction, objection, solely automated processing and the reasoning underlying data processing as enshrined in Article 9 of Convention 108+. National Platforms must also ensure that they have the appropriate technological and organisational systems in place to respond to data subjects' requests regarding those rights. For example, they must ensure that they have the ability to conduct both narrow and wide searches of data so that they can respond to data subjects' access request in an accurate and complete manner. Platform members may need to reorganise their data processing activities in order to comply with requests from data subjects regarding their rights.

Guidance

Two data subjects, both concerned about the accuracy of their personal data which a National Platform member holds, make a request to access their personal data. The first data subject, a regular bettor at a sports gambling shop which is a member of the National Platform, wants to know if the member holds her personal data that relates to the frequency and type of sports bets she places, and whether that personal data is accurate. The second data subject, an athlete that competes on his national gymnastics team, wishes to assess the extent of the personal data on him that has been processed by the national gymnastics federation, which is also a member of the National Platform. The Platform members must have systems in place to respond to, and process, these requests. This may involve the use of specialised software that connects to the databases containing personal data, contains a search function, and returns results in an understandable and comprehensible format. If appropriate, the members may wish to reconsider how they process and store personal data to allow them to better respond to requests from data subjects.

7. Disclosures of Personal Information

The principle of disclosure restricts National Platform members so that they may only disclose personal data to other members of the same National Platform where the disclosure is made to further the goals of the Macolin Convention to eliminate sports manipulation and is made in accordance with applicable data protection laws and the Standard, unless there are other compelling grounds for the disclosure and appropriate safeguards and guarantees provided for by law have been put in place.

Additionally, the principle limits National Platform members to only disclosing personal data to other stakeholders (who are not members of the National Platform) on a case-by-case basis and only if the disclosure has a legitimate purpose. There must be lawful grounds for making any such disclosure, for example where required by law (such as to law enforcement, tax, immigration or other authorities in connection with the performance of their statutory functions or as part of a compulsory legal process such as a court order), protect the interests of the National Platform, or with the free, specific, informed and unambiguous consent of the data subject concerned. Such disclosures must only contain the minimum amount of personal data necessary to achieve its purpose.

National Platform members can more easily comply with this principle through the use of safeguards such as cooperation agreements and memoranda of understanding, provided that they contain an appropriate level of protection of personal data. However, Platform members must not disclose personal data where they reasonably believe the recipient cannot or will not comply with the Standard's data protection principles.

Guidance

A sports team, which is a member of the National Platform, has received a request from a sports betting operator, also a member of the National Platform, to disclose certain personal data relating to the team's staff and players. The sports team may only disclose the personal data if the disclosure reasonably relates to furthering the goals of the Macolin Convention, for example if it is in connection with a reasonable suspicion or documented intelligence of sports competition manipulation, and if the sports team can follow the principles contained in the Data Protection Standard.

The same sports team has received a second request for the disclosure of personal data from an organisation which is not a member of the National Platform. The sports team has determined that it is not required by law to make the disclosure, that the disclosure would not protect the interests of the National Platform, and it has not obtained the consent of the data subjects. The sports team should not make the second disclosure.

As regards international transfers of personal data, the principle of disclosure provides that National Platforms may only disclose or transfer personal data internationally, whether to other National Platforms or third parties, where the disclosure is made in accordance with applicable law and where there is assurance of an appropriate level of protection of personal data based on the provisions of Convention 108+, guaranteed in the laws of the receiving State, or by approved standardised or otherwise ad-hoc safeguards contained in legally binding and enforceable agreements.

In the absence of appropriate safeguards, international transfers and disclosures of data may still take place if the data subject has given free, specific, informed and explicit consent, preferably in writing, and has been informed of the risks of data transfers in the circumstances, as well as in other situations as set out in the Standard.

Guidance

A National Platform member of one State party to the Macolin Convention has received a request from a National Platform member of another State to disclose and transfer personal data.

The first member has determined that the disclosure can be made in accordance with its national law, which allows it to carry out Macolin Convention-relating processing and make international transfers of personal data in furtherance of the Macolin Convention, so it may lawfully make the disclosure. The second member is located in a member State of the European Union and must comply with the European Union's General Data Protection Regulation when processing personal data, so the laws of the receiving State provide an adequate level of protection of personal data.

As the conditions for making an international transfer of personal data are met, the first National Platform member may transfer the personal information to the second National Platform member.

The first National Platform member has also received a substantially similar request from a third party located in a receiving State that does not have laws that guarantee an adequate level of protection of personal data. The member may still make the international transfer of data to the third party provided that it implements further controls to guarantee the same level of protection of personal data. For example, it could enter into a contractual agreement with the third party that obliges the third party to adopt particular data protection measures when processing data received from the member, including not disclosing the data to national law enforcement authorities where fulfilling the request would not be compliant with the applicable data protection requirements, and provides other safeguards.

8. Data Security

The principle of data security requires National Platforms to implement appropriate administrative, technical, and physical measures to protect personal data from accidental or unauthorised access, destruction, loss, use, modification or disclosure. The measures that National Platform members take to comply with this principle must take into account the state of current technology, the costs of implementation, the nature of the processing which the members are performing, as well as the risks and possible harms that might affect individuals if there is a breach of security.

Where a breach of security occurs, the affected Platform member must determine, jointly with the data protection Supervisory Authority where applicable, whether that breach has created a risk to the affected data subjects. If it determines that such a risk exists, the member must notify the competent data protection and law enforcement authorities as required by law. If the risk is serious, it must also inform the affected data subjects as soon as possible.

Guidance

A National Platform member is considering several measures to protect the personal data it processes and stores. When deciding which of these measures to implement, it must not consider only the cost of each measure or the total cost of implementing some of all of the measures, but also consider the state of the art and the risks arising to data subjects in the event of a breach. It must also be aware of its obligations to notify the competent data protection and law enforcement authorities, as well as data subjects where applicable, if a breach of security occurs, and implement measures that enable it to identify a breach and make such notices within any legally mandated time periods.

After some consultation and internal deliberation, the member is deciding between two technological systems that would protect personal data. The first system, which is solely a software solution, is less expensive, easier and quicker to implement, and is a well-known and commonly available product, but has been the subject of criticism due to security vulnerabilities that the developer has promised to fix in the future (but has not yet fixed). The second system provides a combined software and hardware solution that promises extra protection to personal data, but it is more costly. Additionally, as the second solution is fairly new and has not been on the market for very long, it is not a “tried-and-tested” solution and its security efficacy cannot be completely known. The member will need to carefully weigh these factors when making its decision on which of these two systems, if either, to implement.

A few months later, the member suffers a breach of security. Failure to provide the necessary notices within the required time period could give rise to fines and other sanctions for the member.

9. Accountability

To comply with the principle of accountability, National Platform members must take all appropriate measures to comply with applicable data protection obligations, and must keep internal records to demonstrate their compliance with the Standard. This can be accomplished through means such as internal policies and procedures, audit or assessment reports, and the hiring of a Privacy Manager with appropriate data protection experience.

These measures include showcasing 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 measures that a member introduces can be adapted according to the nature and volume of the data it processes, the nature, scope and purpose of the processing, and where appropriate the size of the controller.

Guidance

A National Platform member is implementing measures to comply with the principle of accountability. Amongst others, it has implemented the following measures:

- Hiring of a Privacy Manager with several years’ experience as a data protection compliance officer in a large organisation;
- Regularly compiling internal reports that include data protection compliance metrics such as the number of data subject access requests, how many of those requests were fulfilled and the average response time;
- Adoption of an internal privacy policy, available on its closed network, that details the member’s processing activities in relation to data obtained internally;
- Written documentation that includes details such as the different types of processing activity and the personal data processed, the reason(s) for processing each type of data, the retention period for each type, who has access to different sets of personal data, and the technical, organisational and administrative measures taken to protect personal data including privacy-by-design and privacy-by-default measures; and
- Performing privacy impact assessments on its data processing activities when it is considering beginning new processing or otherwise expanding its current data processing.