COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 29 May 2019

T-PD(2019)4

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

NATIONAL PLATFORMS AND DATA PROTECTION

Daniel P. Cooper

Partner, Covington & Burling LLP

Directorate General Human Rights and Rule of Law

TABLE OF CONTENTS

The views and opinions expressed in this Report are solely those of the author, and do not represent those of other people, institutions or organisations that the author may be or may not be associated with in a professional capacity. The contents of this Report do not constitute legal advice and shall not be construed or interpreted as such.

1. INTRODUCTION & BACKGROUND

a. Aims, Methodology & Structure of Report

This report (the "Report") has been prepared at the request of the Secretariat of the Council of Europe Committee of Convention 108 ("Committee") to clarify the current status and practices of the National Platforms of the Group of Copenhagen[1] when processing personal data pursuant to the Council of Europe Convention on the Manipulation of Sports in Competitions,[2] also known as the "Macolin Convention" (or "Convention").

More particularly, the Report seeks to clarify whether, and if so how, the Group of Copenhagen's National Platforms are hampered by applicable data protection laws from exchanging pertinent information as contemplated by the Convention. It is hoped that this Report ultimately will help to identify potential solutions to any issues identified so as to enhance cooperation between the Group of Copenhagen members under the Convention without breaching applicable data protection norms.

The Report is based on a data protection survey completed by 14 National Platform Coordinators associated with the Group of Copenhagen and submitted to the Secretariat of the Council of Europe in May 2019. The survey, a copy of which appears as an annex to this Report, requested the Coordinators to explain, among other things, the current legal status of their National Platform, the grounds relied upon when exchanging personal data both within the National Platform and with other National Platforms, and whether data protection laws present challenges therein.[3]

Besides the completed surveys, the Report is based on a review of European-level data protection legal frameworks, notably the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108), as amended by protocol in May 2018; the European Union's General Data Protection Regulation (2016/679); and the European Union's Data Protection Law Enforcement Directive (2016/680). The Report does not attempt to analyse any particular member's data protection, sports, gambling, or criminal law.

The structure of the Report is as follows: it begins by discussing the intersection of the Convention, and National Platforms in particular, with European data protection laws, before describing in Section 2 the most relevant European-level laws at a high level. Section 3 enumerates the data protection issues that appear to be causing the most disruption to National Platforms, based on the submissions by the National Platform Coordinators and an analysis of the laws.

---

[1] The Group of Copenhagen, established in July 2016, is composed of 23 Coordinators of National Platforms designated by their respective countries to establish a National Platform. The role of the Group is to serve as a platform for the exchange of information and expertise relating to the establishment and operation of National Platforms.

[2] The full text of the Convention can be found at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016801cdd7e>.

[3] The Report does not divulge any individual survey responses in order to protect the confidentiality of the submissions, as has been requested. However, it can be noted that the following members responded – Denmark, Finland, France, Germany, Italy, Hungary, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland, and United Kingdom – although the quality of the responses varied widely.

b. National Platforms & Personal Data

The Macolin Convention is a legislative instrument that combats the "manipulation of sports competitions"[4] and protects the integrity of professional sport through the establishment of a cooperative, international framework.[5] The Convention encourages more effective coordination of interested stakeholders, sometimes referred to as the "Macolin Community", and obligates countries to implement and promote common standards and principles to prevent, detect, and sanction those involved in manipulating sports competitions[6].

The unfettered exchange of pertinent information among stakeholders, including public authorities, law enforcement, gambling regulators, sports organizations, and sports betting operators, both domestically and internationally, is core to the Convention's mission. To this end, Article 13 of the Convention expressly requires countries to identify a "national platform", which has a number of responsibilities. These include:

- serving as an information hub, collecting and disseminating information relevant to the fight against sport manipulation to other stakeholders;
- receiving, centralising and analysing information about irregular or suspicious betting and non-betting activities involving sports competitions taking place in the relevant country;
- communicating information about possible breaches of legislation or sports regulations to public authorities, sports organizations and sports betting operators; and
- generally cooperating with the relevant organizations and relevant authorities, including National Platforms established in other countries.

The Convention's drafters were well aware that the work of National Platforms would bring them into potential conflict with applicable local, national or regional data protection laws. Article 2 of the Convention observes that respect for the "protection of private life and personal data" must be ensured; Article 14(1) and (2) obliges countries to adopt any and all necessary measures to comply with relevant national and international data protection laws and ensure that their public authorities and covered organizations respect the principles of lawfulness, adequacy, relevance, accuracy, data security and data subject rights.

---

[4] Article 3(4) of the Macolin Convention defines "manipulation of sports competitions" to mean "an intentional arrangement, act or omission aimed at an improper alteration of the result or the course of a sports competition in order to remove all or part of the unpredictable nature of the aforementioned sports competition with a view to obtaining an undue advantage for oneself or for others".

[5] More information on the Convention and its background can be found in the Convention's Explanatory Report: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d383f>; as well as the latest KCOOS Guidebook at: <https://rm.coe.int/kcoos-guidebook-final-1st-version-22-02-2018/16808ecb66>.

[6] Article 3(1) of the Macolin Convention defines "sports competition" as "any sport event organized in accordance with the rules set by a sports organization listed by the Convention Follow-up Committee in accordance with Article 31.2, and recognised by an international sports organization, or, where appropriate, another competent sports organization".

These Convention provisions were sensible and prudent. First, National Platform participants necessarily must collect, hold and share information that relates to identified or identifiable individuals, or "personal data", some of whom may be suspected of, or found to have engaged in, conduct proscribed by criminal law. Second, the proliferation of data protection laws worldwide makes it likely that many, if not most, National Platforms, and not just those in the Group of Copenhagen, will need to effectively incorporate privacy and data protection considerations into the implementation of the Convention. Without exercising due care, National Platforms and their participants risk breaching data protection laws that are increasingly common and infringing rights that often are fundamental in nature.

2. EUROPEAN DATA PROTECTION FRAMEWORKS

Data protection laws, whose purpose is to regulate the processing of personal data, are increasingly commonplace around the globe, after their first appearance in Europe in the early 1970s. By common consensus, European data protection laws today serve as a benchmark for other countries in light of the robust protections those laws extend to personal data. The Council of Europe and the European Union, having recently transformed their respective data privacy instruments, are responsible for some of the most advanced frameworks in effect.

For the Group of Copenhagen, their National Platforms need to take into account the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), as amended ("Convention 108+"). For those members in the European Economic Area, the European Union's General Data Protection Regulation (2016/679) ("GDPR") and Data Protection Law Enforcement Directive (2016/680) ("Enforcement Directive") are relevant. Although this Report does not discuss any specific country-level laws, including laws implementing the above European-level statutes, national legislative and other measures almost certainly will play a key part in addressing some of the issues outlined in this Report.

a. Council of Europe Convention 108+

The Committee of Ministers of the Council of Europe, during its 128th session, materially amended the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) by means of an amending protocol (Protocol, CETS No. 223) on 18 May 2018. The Protocol modernised the Convention to address the emergence of new information and communication technologies and to strengthen its effectiveness as an instrument of data protection law. International organizations can now also accede to the Convention.

Consequently, Convention 108+ now incorporates many of the core data protection principles that have shaped data protection laws in Europe and elsewhere for the past decades. Convention signatories must enact laws to ensure that the processing of personal data is lawful and satisfies such principles as data proportionality, purpose limitation, and transparency. Convention 108+ also vests a variety of rights in individuals, such as rights of access, rectification, objection and erasure. It also commits "controllers" and, where applicable, "processors" to an accountability principle requiring them to adopt appropriate measures to comply with their legal obligations, incorporates breach notification requirements, and more heavily regulates automated decision making.

b. EU General Data Protection Regulation

On 14 April 2016, the EU adopted the GDPR, which took effect in the EU Member States on 25 May 2018. The EU intended for the GDPR, like Convention 108+, to overhaul the EU's data privacy regime based on EU Data Protection Directive 95/46/EC, which similarly had become outdated with the passage of time, emergence of new technologies and advances in computing. The GDPR also was intended to resolve some of the divergent Member State positions appearing under the Directive and improve coordination among the relevant EU Member State supervisory authorities.

These legislative developments, spearheaded by the Council of Europe and the EU, have brought Convention 108+ and GDPR into much closer alignment, although the two instruments are not identical. Similar to Convention 108+, the GDPR requires controllers to engage in fair and lawful processing of data, respect principles of transparency, proportionality, data minimisation, and data security, amongst others, and comply with data subject rights requests such as access, correction, porting and erasure. In addition, the GDPR sets out a detailed enforcement framework, another concept held in common with Convention 108+, and imposes certain accountability requirements, like record-keeping and impact assessments, upon covered entities.

Member States, meanwhile, have supplemented the GDPR at the national level, by enacting national legislation that facilitates the implementation and enforcement of the GDPR into domestic legislation, as they are permitted and, in some respects, required to do in order to lend substance to certain GDPR rules. In fact, a number of GDPR provisions, including some important exemptions, require expression in EU or a Member State law, such as provisions permitting processing where it serves a "public interest" or is pursuant to a "legal obligation". This is also the case where the processing concerns certain categories of sensitive data, or data relating to criminal offences.[7]

c. EU Data Protection Law Enforcement Directive

The EU enacted the Enforcement Directive in parallel with the GDPR, in order to establish a data protection regime specifically for competent EU Member State authorities processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Enforcement Directive is relevant where Member State authorities which belong to a National Platform process or share information with other state authorities in order to detect or prevent sports manipulations, assuming the relevant conduct is criminalised in those countries. The scope of the Directive extends to bodies, other than traditional law enforcement bodies, entrusted by Member State law to exercise public authority and powers for such purposes.

The Enforcement Directive reflects many principles that appear in Convention 108+ and the GDPR, although it adapts them somewhat to suit the specific enforcement context. For instance, there are broader derogations in relation to the rights of individuals, and heavier reliance on laws and regulations to define permitted uses and disclosures of personal data. The Enforcement Directive also regulates the international transfer of personal data for criminal justice purposes, and the means for lawful transfer are similar to those found in

[7] For this reason, the resolution of some of the issues identified in this Report may require countries to consider implementing domestic legal measures, for instance enacting laws that qualify the detection or prevention of sport manipulation as advancing "important public interests" or, for some public authorities, expressly authorizing the processing of personal data for this purpose. See footnote 11.

the GDPR. EU Member States were expected to transpose the Directive into national law by 6 May 2018, and most, but not all, have done so.

3. SPECIFIC DATA PROTECTION RULES

a. Overview

The European data protection law regimes noted above informed the analysis of the surveys submitted by the National Platform Coordinators (the "Coordinators") for the Group of Copenhagen. Broadly speaking, the Coordinators' responses indicate that most regard their data privacy laws, which would include Convention 108+ and, for many, the GDPR, as hindering their effective implementation of a National Platform. In some cases, Coordinators indicated that their National Platforms are not yet operational, although it was unclear whether this was due to data protection laws specifically or other reasons.

The Coordinators identified a number of data privacy-related concerns, discussed below. This may be due, in part, to the fact that National Platforms contain dissimilar stakeholders reliant upon different legal bases to process personal data, certain stakeholders are required or expected to process sensitive or judicial data, and the Convention expects some cross-border transfer of personal data. It also may be due to the fact that there is limited, if any, regulatory guidance in this sphere and the relevant legal frameworks are new and untested.

It appears that law enforcement, regulatory agencies and similar bodies, authorised by law to prevent or sanction match fixing, illegal betting and related activities, encounter fewer issues, as opposed to private actors, such as betting agencies, event organizers or sports bodies, which cannot similarly leverage laws or regulations to justify their processing. For instance, some Coordinators identified legal provisions appearing in national data protection, gambling or sports laws that specifically authorised certain stakeholders to process data for the purpose of detecting or preventing sports manipulation, helping to surmount data privacy obstacles. Overall, however, this Report concludes that both perceived and actual issues stemming from applicable data privacy law regimes may be disrupting Group of Copenhagen members' efforts to deploy and operate National Platforms.

Coordinators responding to the survey identified some of the following challenges:

- identifying a clear legal basis in data privacy laws that would allow certain National Platform participants to lawfully collect, receive or share data, particularly sensitive or judicial data, with other participants;
- complying with vaguely worded proportionality mandates when collecting, processing or sharing personal data in the context of National Platforms;
- complying with restrictions on the cross-border or international transfers of personal data when providing data to National Platforms in third countries;
- understanding the technical, organizational or physical security measures needed to address data security rules when handling or sharing personal data in the National Platform; and

- operating in the absence of guidance, standards or other tools from national privacy regulators to serve as guideposts for National Platform participants processing data for this particular purpose.

b. Data Protection Rules and National Platforms

3.b.1 Legal Bases: Personal Data

Controllers processing personal data – including collecting and sharing data with third parties – must have a "legitimate" or "legal" basis for the processing. This legal basis may derive from the data protection law itself, where it enumerates a list of permissible processing grounds, or may derive from other laws or regulations, which are then recognised as valid under the data protection law. For example, Convention 108+ allows controllers to process personal data on the basis of consent or another "legal basis laid down by law" [8], calling upon Convention signatories to enact laws enabling the processing of data without consent. For instance, a country's gambling or sports law may authorise certain controller parties to collect, use and share personal data to combat match fixing, subject to meeting certain conditions set out in those laws.

The GDPR goes further and actually identifies a number of legal grounds for validly processing personal data, besides consent, such as where processing is necessary to perform a contract with the individual; where processing is necessary to comply with a legal obligation expressed in a Member State or EU law; where processing is necessary to perform a task carried out in the public interest expressed in a Member State or EU law; or where processing is in the exercise of official authority; and where processing satisfies certain "legitimate interests" provided additional conditions are met. As is evident, the GDPR itself contemplates Member States enacting further laws to help give effect to a few important GDPR provisions.

Turning to the National Platforms, it is self-evident that the relevant participants not only must collect personal data to fulfil their normal roles and functions, but often must disclose and share personal data with others to operate effectively and in the manner envisioned by the Macolin Convention. Article 12 of the Convention states, in particular, that signatories are to "facilitate…exchanges of information between the relevant public authorities, sports organizations, competition organizers, sports betting operators and national platforms"; National Platforms are the chief means by which this is accomplished. This data can include basic information, such as the name, date of birth, IDs and contact details (e.g., phone numbers; email addresses) of individuals, such as members of the public, athletes, support personnel, and officials. It also can include information about betting behaviour, relevant sporting event, location information, financial data, photos and other relevant identifiers of individuals.

National Platform participants sharing data with one another require a valid legal basis to do so to comply with data protection laws. However, the surveys strongly suggest that some National Platform participants are uncertain regarding the appropriate legal basis that permits them to share data with other participants (or, conversely, to process data that other participants may share with them). This uncertainty can extend to the sharing of data with participants of other National Platforms, in a foreign country. Such doubts inevitably weakens the effectiveness of the National Platform and undermines one of the primary goals of the Macolin Convention.

[8] Article 5, CoE Convention 108+.

Matters are not helped by the fact that the different National Platform participants, including law enforcement, government agencies (e.g., gambling regulators), betting operators, sports bodies, sports regulatory bodies and event organizers, generally rely upon different legal bases when processing personal data, as noted above. Police authorities or gambling regulators may be processing data "in the exercise of official authority", whereas a sports body may be relying upon consent or "legitimate interests".[9] The surveys revealed that some national betting operators can be required by law or by the terms of their licence to share suspicious data with police, gambling regulators or others, making it easier for them to share data, but at least one Coordinator indicated that their gambling authority was without any express statutory powers to process such data. Because of concerns over having a valid legal basis, private actors in at least one National Platform will only share data in response to a formal law enforcement request and first invite law enforcement to make the request, adding a layer of administrative complexity.

Compounding the problem, some National Platforms have not been formally established in their countries or, where they have been established, are not recognised in law, leaving their stakeholders without a strong legal basis for actively participating in their National Platforms. Only a small minority of Coordinators indicated that their National Platform had official legal status. Most had no such status, but was more of an informal collaboration of parties.

3.b.2 Purpose Limitation Principle

Closely associated with the above, data protection laws prevent controllers from engaging in new, incompatible processing purposes. Article 5, Convention 108+, for instance, provides that personal data shall not be "processed in a way incompatible with" the original reasons for its processing. The GDPR and Enforcement Directive contains a similar provision. This rule is engaged where National Platform participants find themselves processing data that they collect for one purpose (e.g., administering an event), and then convert it to a new use (e.g., detecting match fixing). A member's original legal basis for processing certain personal data can and often does confine the organization's ability to put it to another use, unless another legal basis can be identified. For example, processing personal data on the basis of an individual's consent is limited by the scope of that consent. Processing based on a law is allowed, but only to the extent the law actually requires the data to be processed.

It appears from the surveys that most public authorities, such as law enforcement bodies or regulatory agencies, rely on legislation that explicitly permits their processing of relevant data to fulfil their individual legal mandates. Private actors, such as sports bodies, gambling bodies and the like, however, have a more challenging situation under data privacy laws, unless Convention member countries have adopted targeted measures that they can leverage.[10] For this reason, it is unsurprising that private actors are able to share

[9] Article 6(1)(e), (a) & (f), EU GDPR.

[10] Some Coordinator responses indicate that, in at least some countries, domestic legislation has been introduced, or existing data protection, sports, gambling or other laws amended, to specifically facilitate the free flow of data within or between National Platforms to address this issue. In the EU, this development could allow National Platforms members to take advantage of additional, more robust legal grounds for processing data, such as compliance with a legal obligation or performance of a task in the public interest. The UK's Data Protection Act 2018, for example, expressly provides that, subject to certain conditions, any parties processing data, including sensitive data, to "protect the integrity of a sport or sporting event" satisfy the "substantial public interest" legal basis set forth in the law. This promotes the processing and sharing of

data with public authorities tasked with eliminating bribery, corruption and other conduct associated with sports manipulation, but data – especially sensitive data – does not flow as readily in the other direction.

3.b.3 Legal Bases: Sensitive and Judicial Personal Data

Any concerns regarding an appropriate legal basis are exacerbated where National Platform participants process sensitive or so-called "judicial" data, which can easily occur where countries criminalise the manipulation of sport through their domestic sports laws, criminal codes and even via bespoke legislation.[11] Such data, which includes information relating to a person's commission of an offence, is more highly regulated and permits of fewer legal bases, reflecting the greater privacy risks.[12] Where National Platform participants are exposed to such data, whether through their own collection or through receiving it from other members, concerns relating to legal basis take on a greater intensity as a result.

Under the EU's Enforcement Directive, for example, public authorities may only collect, use and share judicial data when permitted by law and in order to prevent, investigate, detect or prosecute criminal offences or execute criminal penalties.[13] Under Convention 108+, the processing of sensitive data is allowed if additional safeguards complementing those of Convention 108+ have been put in place.[14] The GDPR, in turn, makes data relating to criminal convictions and offences its own unique sub-category of data, and limits it processing to where it occurs under the control of "official authority" or where EU or Member State laws expressly permit it.[15]

Once again, law enforcement authorities, government agencies and comparable entities, which are mandated by law to investigate criminal conduct, experience fewer issues processing sensitive or judicial data, as it generally falls within their statutory powers to receive, process and even share such data. Conversely, private actors have greater concern as they frequently cannot point to any clear legislative language or other "safeguards" "enshrined in law" to legitimise their processing of such data. Coordinators in only a minority of countries indicated that they had such measures in place already or that were pending.

---

personal data for this purpose. Norway and Switzerland, amongst others, also have introduced specific legislative measures to alleviate the tensions between the Macolin Convention and data protection laws.

[11] For a comprehensive, albeit dated, analysis of such laws, see https://www.unodc.org/documents/corruption/Publications/2017/UNODC-IOC-Study.pdf.

[12] Article 6, CoE Convention 108+.

[13] Article 8, EU Enforcement Directive.

[14] Article 6(1), CoE Convention 108+.

[15] Article 10, EU GDPR.

3.b.4 Proportionality and Necessity

European data privacy laws require that controllers, whether public or private actors, engage in "proportionate" processing of personal data, and avoid the collection and processing of any personal data that is not strictly necessary to fulfil their stated purposes or aims. Under Convention 108+, data undergoing processing must be "adequate, relevant and not excessive in relation to the purposes for which they are processed". This proportionality requirement is expressed nearly identically in Convention 108+, the GDPR and the Enforcement Directive.[16]

Some Coordinators identified the proportionality principle to be a concern where participants process or share data with others involved in the National Platform. Proportionality concerns are frequently raised by organizations subject to the GDPR, as the law is necessarily imprecise and provides data privacy regulators with a convenient basis for launching investigations and sanctioning conduct. As a result, it is not surprising that some National Platform participants are cautious about what information they are willing to process to address sports manipulation.

3.b.5 International Transfers of Personal Data

Restrictions on international data transfers are found in each of the European frameworks under consideration here. These restrictions can generally be overcome where the third country to which data are to be sent offers an equivalent or "appropriate" level of protection, where the relevant parties execute contractual or other controls to govern the transfer, or where there are applicable derogations, such as where the transfer occurs with the consent of the individual or serves important public interests.[17]

National Platforms operating in countries subject to Convention 108+ should be able to transfer data with one another, unless there is a "real and serious risk" that the transfer would lead to circumvention of provisions of the Convention. Further, the Convention also provides that parties may refrain from transferring data where their regional laws, like the EU's GDPR or Enforcement Directive, impose additional restrictions, meaning that National Platforms in some Group of Copenhagen countries will also need to take these additional rules into account.[18] The Macolin Convention's provisions calling for exchanges of information at international levels triggers these data transfer rules especially.

The survey identified some transfers of personal data by National Platform participants to entities outside of Europe, and only a limited number of transfers within Europe (most transfers appear to take place within the EU and with sports bodies located in Switzerland). As a result, National Platforms have yet to encounter significant problems with international data transfers, but are likely to do so once they begin to share data with National Platforms situated outside of Europe. A number of Coordinators noted that memorandums of understanding ("MoUs") are used to transfer data, and many send only redacted, non-identifying information to further reduce the data privacy risks. Transfers to National Platforms in a Convention 108+ country also may need to consider whether

[16] Article 5.4(c), CoE Convention 108+; Article 5(1)(c), EU GDPR; Article 4(1)(c), EU Enforcement Directive.
[17] Article 14 (3), CoE Convention 108+.
[18] Article 14(1), CoE Convention 108+.

additional controls might be required, where the recipient National Platform is not in the EEA or an "adequate" jurisdiction, like Switzerland.

If transfers to National Platforms in other regions are to take place in future, Convention 108+ requires that additional steps be taken to protect the data, for example, through a law authorising the transfer or through legally binding and enforceable instruments.[19] Transfer restrictions under the GDPR and the Enforcement Directive are similar, although formulated somewhat more strictly than under Convention 108+. In addition, access to any data by foreign law enforcement bodies to personal data originating in Europe remains a highly controversial topic, as evidenced by current debates surrounding the Second Additional Protocol to the Budapest Convention as well as recent legal challenges to the EU-U.S. Privacy Shield Framework and EU model contractual clauses.

3.b.6 Data Security and Related Concerns

European data privacy laws require controllers to apply "appropriate" security safeguards to personal data, which take into account the risks that the processing represents to the relevant individuals, the technical security measures available at the time and other factors, and can require prompt reporting of any data security breaches to data privacy authorities and individuals. For sensitive data categories, more rigorous security measures are required, and encryption is ordinarily used for data transfers. Although these frameworks do not require adoption of any particular security standard, seal or code, certain safeguards, such as technical standards released by ENISA, ISO/IEC, CEN/CENELEC, and ETSI are available and often popular.

Few Coordinators identified data security to be a particular concern, although this is likely to be an issue for many National Platforms in due course, where they do not have a dedicated and secure platform or network for the collection and dissemination of data. Some Coordinators indicated that their law enforcement bodies and regulatory agencies were able to use specially dedicated networks to communicate with each other, which is encouraging. Where this is not the case, it has to be assumed that more conventional, and often less secure, means of sharing data are used. With many National Platforms still in the early stages of development, few appear to have dedicated tools or technology platforms allowing for the secure sharing of data amongst the relevant participants. The secure transmittal of such data is vital to compliance, particularly in the context of sensitive and judicial data. In time, these may become essential in allowing participant members to share data in a controlled and secure environment.

3.b.7 Other Issues

Although not raised in the surveys, there could be other data protection law concerns warranting consideration by National Platform Coordinators. For instance:

- Transparency: Convention 108+, the GDPR, and the Enforcement Directive require controllers to be transparent about their processing of personal data, often manifested in a form of notice or privacy policy presented to the individual. It is unclear to what extent National Platform members satisfy these requirements, or alternatively rely upon a recognised exemption, such as the exemption in the GDPR where such notice would involve "disproportionate effort".

[19] Article 14(3), CoE Convention 108+.

- Data deletion: One aspect of the European data minimisation principle is that data are deleted promptly, and only "preserved in a form which permits identification of data subjects for no longer than is necessary"[20]. The issue of when National Platform participants should begin to delete the data they process purely to serve the purposes of the Macolin Convention is likely to become an issue in time, if it has not already, and there appears no emerging standards or consistent practices.

- Data subject rights: Convention 108+, the GDPR, and the Enforcement Directive bestow rights upon individuals, including rights to access, correct and erase their data, as well as to object to its processing. The Coordinators surveyed did not set out in any detail how members were ensuring compliance with such rights as a practical matter and it may be that there have been few data subject rights requests to date. Given the nature of the processing and its impact on individuals, it is likely that access and erasure demands will become more common.

3.b.8 Engagement with Regulatory Authorities

At this stage, there is evidence of limited constructive engagement between the National Platforms and their data privacy authorities, which might help clarify regulatory expectations in this field and remove obstacles. Some Coordinators indicated that regulators were aware of their activities or that they had links to regulators of some sort. In at least one case, a national data privacy authority appears to have drafted a report and may have shared it with the National Platform. These relationships generally have not matured to the point where regulators are providing National Platforms with tailored guidance and advice regarding data protection issues. Continued engagement may help to educate authorities about the aims of the Macolin Convention, so that they are more sympathetic to the needs of National Platform participants, familiar with their concerns and able to effectively advise stakeholders on their data protection responsibilities.

4. CONCLUSIONS

National Platforms inspired by the Macolin Convention, and dedicated to the eradication of sports manipulation, must account for a number of well-established data protection rules. This is inevitably the case where multiple parties collaborate in the collection and sharing of information, particularly as between private and public entities. Concerns here may be higher than normal given the purposes served by the National Platform, the sensitivity of the data and the fact that international transfers will take place. The fact that Convention 108+, the GDPR and Enforcement Directive are all new legal instruments whose rules largely remain untested before courts, in addition to the relative lack of guidance as to their implementation, is contributing to the problem. Also unhelpful is the fact that most of the countries surveyed do not yet appear to have attempted, as yet, to enact any specific measures to counter-balance these concerns and help clarify the lawfulness of the processing of personal data by National Platform members.

[20] Article 5.4(e), CoE Convention 108+.

DIRECTORATE GENERAL OF DEMOCRACY

Directorate of Anti-Discrimination
Sport Conventions Division

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
1949.2019

Strasbourg, 24 April 2019 T-MC(2019)34

Convention on the Manipulation of Sports Competitions (Macolin Convention)
Network of the National Platforms (Group of Copenhagen)

Data Protection

Questionnaire

Introduction

The Group of Copenhagen [7th plenary meeting, Oslo, 18-20 February 2019, see Aide Mémoire T-MC(2019)25fin] committed to work on Data Protection issues "*in order to clarify as quickly as possible what the National Platforms can and must do in the current legal environment, and also to identify the urgent measures to be taken to make the Macolin Convention fully operational once it comes into effect*".

An Action Plan 2019 [T-MC(201932] has been proposed. Actions will be implemented by the Secretariat of the Council of Europe, in coordination with the Council of Europe Committee on the CETS Convention n° 108.

The first step of the process aims at:

- Clarifying the state of the art, and identify benchmarks for exchanging information by National Platforms
- Gathering basic, data-protection related information from NPs and producing a "diagnosis"

The Secretariat of the Council of Europe has prepared the following questionnaire addressed to the member countries of the Group of Copenhagen.

Replies should be addressed to the Council of Europe secretariat (mikhael.dethyse@coe.int) at latest by 7 May 2019 (close of business).

Relevant legislative references:

- Article 14, Convention on the Manipulation of Sports Competitions CETS 215
- Convention for the protection of individuals with regard to the processing of personal data (Convention 108+)
- Practical guide on the use of personal data in the police sector (Convention 108+)
- Definition of "personal data" and "processing data" (Article 2, Convention 108+)

Questions	Answers
1. What is the legal status of the NP? If not official, what is the plan for legal status?	

2. What legislative basis (i.e., what law, regulation, etc.) do you have for national exchange of personal data (please refer to the definition in Convention 108+) between:	
a. public authorities (ministries, betting regulatory authority, law enforcement agencies, prosecutor's office – please specify all that exist nationally)	
b. public authorities and private entities: **i.** sport organisations (which sport organisations – competition organisers as well as other federations, athletes' associations, referee unions, etc) **ii.**betting operators – please specify which operators and agreements	
c. the above mentioned private national entities	
3. Trans and international exchange of personal data (please refer to the definition in Convention 108+):	
a. What legislative basis do you have for exchange between private national organisations and international private entities - international sport federations, monitoring systems and companies, associations, etc. Please specify if this includes National platforms depending on the public/private status of your NP.	
b. What legislative basis do you have for exchange between public national authorities and international private entities - international sport federations, monitoring systems and companies, associations, etc. please specify if this includes National Platforms depending on the public/private status of your NP.	
c. Do you have and/or use other data exchange international regimes other than the Macolin Convention? Please specify	
4. What are your practices in relation to exchange of information (personal data and otherwise please specify) nationally- What information do you exchange and with whom?	
5. What are your practices in relation to exchange of information trans-	

and inter-nationally? What information do you exchange? With whom (other NPs, international level entities, private and public)?	
6. What legal mechanisms, if any, do you use when transferring information trans and inter-nationally (e.g., contracts, MoUs)?	
7. What are the types of personal data that you normally process? (please refer to definition of personal data and processing above) – this includes storing, collecting, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of, or the carrying out of logical and/or arithmetical operations on such data.	
8. What is your legislative basis for collecting and processing personal data, or is it the same legislation identified under Q. 2 and 3 above?	
9. Do you process any personal data that is "special" or "sensitive" under your data protection law regime, such as data relating to criminal offences? Please describe.	
10. What, if any, are the chief barriers to collecting or sharing personal data within your NP or with another NP under your data protection law regime? Please explain how these are barriers.	
11. Is the supervisory authority for data protection involved with or aware of your National Platform? Please specify/detail.	
12. Do you have specific record-keeping or other requirements when processing personal data under your National Platform?	