Implementing the GDPR in Switzerland: legal issues and challenges for international sports bodies

Print

Published 30 May 2019 | Authored by: Dr. Jan Kleiner, Carol Etter

This article describes legal issues and challenges currently arising for international sports bodies domiciled in Switzerland when implementing the General Data Protection Regulation (**GDPR**), which came into effect on 25 May 2018.

Approximately one year after its entry into force, the GDPR still causes various legal questions for sports bodies, some of which still need to be clarified. The article provides a short overview on practical implications and possible legal issues, and aims to provide guidance on how such challenges can be addressed.

SPORTS LAW ADVISORS

SPORTS LAW COURSES

UPCOMING EVENTS

JUN 28

MedEduCare update day on Anti-doping - Medico-legal issues

Conference

London

SEP 12

Understand The Rules Of The Game 2019 - LawInSport Annual Conference

Conference

APPLICABILITY OF THE GDPR IN SWITZERLAND

At the outset, it must be clarified whether and when the GDPR applies to a sports governing body domiciled in Switzerland. As it is commonly known, the GDPR is a Regulation established by the European Union, of which Switzerland is not a Member. The (wrong) impression may therefore exist that the GDPR would generally not apply to parties based in Switzerland.

However, the geographical scope of application of the GDPR goes beyond the territory of the EU. In particular, the GDPR applies to all parties that offer goods or services directed at a person (a "*data subject*") domiciled in the EU, irrespective of whether the party offering goods or services is domiciled itself in the EU and irrespective of whether or not a payment is required. Accordingly, whenever a sports body offers its services or its governing functions to Athletes or Clubs domiciled in the EU, this is very likely to trigger the applicability of the GDPR.

Other aspects of the work of sports governing bodies may also very quickly become subject to the material obligations arising under the GDPR. It is sufficient, for example, to operate a website, which is directed towards users in the EU.[1] This will trigger all data processing activities occurring on that website to fall under scrutiny under the GDPR.

Finally, whenever a "*Controller*"[2] uses services of a third-party "*Processor*"[3] domiciled in the EU, the material data processing obligations, in particular for such third-party processing, arising under the GDPR will apply as well, regardless of whether the processed data affects data subjects in Switzerland or in the EU.[4]

It is therefore evident that sports bodies based in Switzerland will very quickly meet the criteria for the application of the GDPR. Not only do sports bodies have affiliated members domiciled in the EU, but they also organise competitions within the territory of the EU, process data of Athletes domiciled in the EU, offer services to sports officials of EU countries, etc. For all these reasons, sports governing bodies are well-advised to carefully assess the extent to which their data processing

activities are governed by the GDPR and which obligations arise therefrom. In particular, sports bodies in Switzerland must ensure that their global data exchange and transmission models are able to meet these high regulatory requirements. The potential legal and financial exposure is considerable, especially for legal entities that process so-called "*sensitive personal data*" (such as, for example, health data of athletes).[5] Not least is the threat of heavy sanctions in case of breach, which makes it clear that GDPR compliance should be a top-level priority for all international sports federations.

OBLIGATIONS UNDER THE GDPR: OVERVIEW

With the entry into force of the GDPR on 25 May 2018, various new legal obligations arose for a Controller and a Processor of personal data. The (controversial) level of possible sanctions for breach underlines the importance of GDPR compliance: fines of up to EUR 20 million or, if higher, of 4% of a company's worldwide turnover in case of a breach of the regulations.[6]

Switzerland also faces the added complication that its current national data protection laws are partially less restrictive than the GDPR, meaning the GDPR imposes various additional operational requirements that do not exist as such under the current national data protection regime.

ORGANISATIONAL REQUIREMENTS: GENERAL REMARKS

The GDPR can be quite overwhelming as the law text itself might not give away how extensive the implementation of each and every requirement is.

Many (sports) organisations have been facing the complex challenge of undertaking a compliance review, often in the form of an initial gap analysis, to identify whether – and if so, to which extent – data processing activities must be changed or amended in order to become GDPR-compliant. These often burdensome tasks may range from a rather simple increase in documentation requirements up to a full re-modeling of the IT infrastructure or, for example, of the results management processes of sports federations.

When addressing GDPR compliance, there are, first of all, general purposes, which need to be applied in a general manner and must be kept in mind for every processing of personal data. One of the key purposes of the GDPR is the reduction of data processing to a minimum: Only such data may be processed as it is strictly necessary in relation to the purposes for which the data is processed.[7] Data must only be collected for specified, explicit and legitimate purposes and must not be processed for other purposes.[8] Data may only be stored as long as it is needed[9] and must be accurate and up to date.[10] Finally, data must be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage.[11]

On the other hand, there are specific (new) requirements such as the implementation of a processing directory and the conclusion of certain types of agreements, which may need to be created from scratch.

In practice, various organisational measures must be adopted. The below considerations describe some of the important organisational requirements that must be addressed by sports governing bodies to ensure GDPR compliance. However, it must be noted that additional requirements may exist and a careful case-by-case analysis is recommendable for each sports federation which processes personal data.

ORGANISATIONAL REQUIREMENTS IN DETAIL

APPOINTING AN EU REPRESENTATIVE

Controllers and Processors domiciled in non-EU Member States, which fall under the scope of the GDPR, must designate a representative in one of the Member States where at least one of the concerned data subjects is located.[12] A mandate must be concluded with this representative, but there is no general reporting obligation as to which entity or person has been appointed. The practical significance of this obligation is until today rather unclear: In particular, the exact role of this representative still needs to be clarified in practice. Additionally, for sports federations processing

data in many EU Member States, not much guidance exists in which of these states a representative must be appointed.

PRIVACY POLICY

For all websites operated by sports governing bodies, having a state-of-the-art privacy policy is certainly a key element to demonstrate compliance with the GDPR. Such a privacy policy can very well be used by supervisory authorities as a first indication of whether a closer examination of data processing activities and of GDPR compliance may be warranted or not. If it is already obvious based on a very poor privacy policy that GDPR compliance seems to be low, this may quickly trigger closer investigations.

As to the required content of a privacy policy, it must be noted that such a policy must always provide information on the type, scope and purpose of the collection and use of personal data.[13] The legal basis for data processing must always be mentioned with a precise reference to the GDPR.[14] Users must be informed in detail about their rights, which include:[15]

- A Right of objection to data processing /right to revoke consent
- A Right of access to data
- A Right to have data rectified or deleted or the processing of data restricted
- A Right of appeal to a supervisory authority
- A Right to data portability

The user of a website must not only be informed about who receives the personal data collected, but also whether the data is transferred outside the EU (and, if so, which measures have been put in place to meet applicable data protection standards). Furthermore, a user must know how long his data will be stored and if so-called automated decision-making processes exist. Finally, every privacy policy must include contact information of the entity responsible for the processing of data.

PROCESSING DIRECTORIES

Each Controller of data has to maintain a record of its processing activities, which has to, among other things, include the purpose of the processing, a description of the categories of data subjects, categories of personal data, categories of recipient and if personal data is transferred to third countries the documentation of suitable safeguards.[16]

PROCESSING AGREEMENTS

Whenever personal data is transmitted to third parties which process data on behalf of the Controller, the Controller is required to contractually bind the service provider to the regulations of the GDPR and to conclude a rather detailed data processing agreement.[17] While standard templates exist for such contracts, the key challenge for sports entities may be, in a first step, to identify all the constellations in which it uses third-party Processors and to conclude data processing agreements wherever necessary. Once these agreements are concluded, it must be noted that a Controller should maintain a list of all its third-party processors and regularly monitor their GDPR compliance, since the ultimate legal responsibility for possible breaches of these processors remains with a Controller.[18]

TECHNICAL AND ORGANISATIONAL MEASURES

Each Controller and Processor must implement "*appropriate technical and organizational measures to ensure a level of security appropriate to the risk*" of their data processing activities. In essence, this means that each Controller and Processor must make sure to implement a state-of-the-art IT security system and carefully document all steps taken to ensure the technical security of their data processing activities.

A Controller must furthermore implement appropriate technical and organizational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is indeed processed. This obligation applies to the amount of data collected, the extent of its processing, the period of its storage and the accessibility of data (so-called principle of "*Data Protection by Design and by Default*").[19]

In order to demonstrate compliance with the principles of data protection

by design and by default, a company should adopt internal policies and implement measures. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing and enabling the controller to create and improve security features.[20]

GENERAL IMPORTANCE OF DOCUMENTATION

As a final remark, it must be noted that for any sports governing body, and indeed for any entity processing data under the GDPR, documentation in all aspects remains key: In the scenario where suddenly, data processing activities come under scrutiny by a supervisory authority, it is ideal for a Controller if it is immediately able to produce a detailed, thorough and up-to-date documentation of all its processing activities, the legal permissions on which it relies and of all the measures it takes to be GDPR compliant. If such a documentation can be immediately produced, it will not only show a supervisory authority that the obligations under the GDPR have been taken seriously, it will also facilitate the clarification of any queries which a supervisory authority may have.

IDENTIFYING THE SPECIFIC LEGAL GROUND ON WHICH A SPORTS BODY MAY BASE ITS DATA PROCESSING ACTIVITIES

One of the key requirements of the GDPR for lawful data processing is the need for a legal permission for all processing activities. In practice, it may be difficult to identify the specific legal ground on which a sports body may base its processing activities.

According to the GDPR, data may be processed under one of the following circumstances (legal permissions):

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;[21]
- processing is necessary for the performance of a contract to which the

data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;[22]

- processing is necessary for compliance with a legal obligation to which the Controller is subject;[23]
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;[24]
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;[25]
- processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[26]

For some processing activities, specific state legislation may exist, notably in the fight against doping.[27] However, for other processing activities, no such legal permissions may exist. Apart from scenarios where data processing activities directly relate to a contractual relationship between, for example, a federation and an athlete, sports governing bodies will often have to rely either on a "*legitimate interest*" [28] or on the consent of the concerned data subject[29].

However, both of these possible legal permissions may be challenging to apply in practice.

CONSENT

It may be debatable whether consent given by an athlete is considered as valid in all circumstances. In many aspects of its activities, a sports governing body holds a very strong position towards an athlete (or coach, official, etc.), i.e. it acts as an authority with legal powers. Every athlete wishing to participate in organized sports, within its pyramid structure, must submit himself/herself to the binding regulations enacted by sports bodies.[30]

The GDPR, however, defines consent as

> "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"[31].

The expression "*freely given*" implies that voluntariness of consent is a strict requirement for the validity of consent, which is also widely discussed – and largely confirmed – in legal doctrine.[32] Many authors question the validity of consent given by athletes in light of the "*imbalance*" between an athlete and a sports federation. For an athlete, it is usually a "*take it or leave it*" situation, which means that he/she is unable to refuse or withdraw consent to data processing (and other regulatory or legal obligations) without detriment.[33]

However, the aspect of the imbalance and consequently the invalidity of a consent given when it comes to bargaining power or market position may need to be looked at differently in the context of organized sport. Simply referring to an imbalance between the stakeholders and assuming that, based on a "*free*" choice, an athlete would possibly not give his/her consent is, in the authors' view, mistaken. Many data processing activities in organized sport do not only serve the interests of the sports federations, but just as importantly also the interests of athletes. For example, data processing in the fight against doping or in the context of sports governance and the management of a sports overall most certainly also directly serves interests of athletes. It can therefore be validly assumed that there is no situation of general imbalance, which would somehow force athletes to give a consent, which they would otherwise not do.

Accordingly, considering any and all consent given by athletes towards a sport federation as generally invalid appears incorrect. Rather, a careful case-by-case approach should be taken to assess whether, in specific circumstances, an athlete may be de facto forced to give consent, which he/she would not have given if the imbalance did not exist. Only in such a scenario, consent should be considered as invalid.[34]

LEGITIMATE INTERESTS

In practice, legitimate interests may often be a more reliable legal permission for sports federations, in particular in view of the general criticism towards the validity of consent.

Indeed, relying solely on consent may cause additional practical obstacles for sports federations: A sports body would have to be able to document each and every consent it has ever received. Moreover, consent given by an athlete can be revoked at any time – which may cause a high degree of uncertainty if processing activities can only be based on consent.

While there are, as mentioned, good arguments for the validity of consent given by athletes, most of those arguments also apply for the legal permission of legitimate interest. In essence, wherever data needs to be collected, processed and published for the proper functioning of a sport, a sports governing body may very likely invoke legitimate interests in the respective processing activities.

Although there is little to no case law, which would provide specific guidance on the balancing of such interests, it is the authors' view that in general, it can be assumed that such interests of sports governing bodies will generally outweigh the interests or fundamental rights of the athletes concerned as data subjects. For example, any sports governing body has a very legitimate interest that it needs to be able to process personal data of athletes or players, because otherwise, it could not fulfil its role as governing body. For example, an international sports federation needs to be able to collect, store, catalogue, communicate etc. all the individual results and records achieved by athletes in its sport, because only by doing so, results are truly comparable. Likewise, a sports federation must be able to collect date on sanctions, possible doping offences, transfer movements, etc. of all participating players and athletes, because without such information, a sports federation could not exercise its governing functions in the first place.

All of this is, ultimately, not only in the interest of the governing body, but also of each individual athlete or player, who benefits from these governing functions.

If there are arguments for both consent and legitimate interest, the latter may therefore often be the better choice. An important aspect to bear in mind for a sport body is to carefully document the findings for the legal

permission and stick to those findings. It is either asking for consent or relying on legitimate interests. It is generally forbidden, for example, to first ask for consent, and if not given or revoked rely, as a fall-back option, on legitimate interests.

SUMMARY AND OUTLOOK

The GDPR is an important set of rules for all sports governing bodies domiciled in Switzerland. Although Switzerland is not a Member State of the European Union, data processing activities of such sports governing bodies may very likely fall within the scope of application of the GDPR.

Therefore, and in particular in view of potentially very heavy sanctions applicable in case of breach[35], sports governing bodies are well advised to ensure compliance with the GDPR for all their data processing activities and to perform, if this has not yet been done, a careful analysis of its current practices.

The GDPR imposes various organisational requirements, in particular detailed documentation obligations, obligations related to technical and organisational measures, the appointment of an EU representative, and others. From a purely legal perspective, an additional challenge for sports governing bodies consists of the legal permission for data processing activities. While there are good arguments that consent given by athletes can be considered as valid, reliance on legitimate interests may in practice often be the preferred legal permission.

Moreover, one must bear in mind that the current Swiss Data Protection Act (DSG) is undergoing a process of revision. On 15 September 2017, the Federal Council adopted the introductory comments on the revision of the Data Protection Act. Already at this stage, it is clear that the future amendments to the Swiss DSG will very closely follow principles established under the GDPR. Most importantly, it seems unlikely that the amendments to Swiss data protection law would go further than what the GDPR already provides for. Therefore, a sports governing body which today aims at full GDPR compliance, can be reasonably assured that by doing so, it will already be compliant to a very large extent with any future developments in Swiss law. However, once the new DSG will enter into effect, a careful review of data processing activities also from the angle of

Swiss law certainly remains recommendable.

References

[1] It is stated, for example, that whenever a website uses a language or offers goods/services in a currency other than the one of the domicile of the party operating the website (notably languages or the currency of the EU), the website targets data subjects domiciled in the EU; see Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation by the European Data Protection Board (edpb), adopted on 16 November 2018, p.12 et seqq. (2 a and b).

[2] The role of a “Controller” refers to a natural or legal person, public authority, agency or other body which (alone or jointly with others) determines the purposes and means of the processing of personal data (Art. 4 para. 7 GDPR).

[3] The role of a “Processor” refers to a natural or legal person, public authority, agency or other body which processes personal data on behalf of a Controller (Art. 4 para 8 GDPR).

[4] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation by the European Data Protection Board (edpb), adopted on 16 November 2018, p.8 et seqq. (1 c).

[5] See Art. 9 GDPR.

[6] Art. 83 GDPR.

[7] Principle of “data minimization”, art. 5 para. 1 c) GDPR.

[8] Principle of “purpose limitation”, art. 5 para. 1 b) GDPR.

[9] Principle of “storage limitation”, art. 5 para. 1 e) GDPR.

[10] Principle of “accuracy”, art. 5 para. 1 d) GDPR.

[11] Principle of “integrity” and “confidentiality”, art. 5 para. 1 f) GDPR.

[12] Art. 27 GDPR.

[13]

Art. 12-15 GDPR.

[14] The legal basis for the permission can be found in Art. 6 GDPR.

[15] Art. 16-20 GDPR.

[16] Art. 30 GDPR.

[17] Art. 28 GDPR.

[18] See Art. 28 GDPR.

[19] Art. 25 GDPR.

[20] GDPR, Recital 78.

[21] Art. 6 para. 1 (a) GDPR.

[22] Art. 6 para. 1 (b) GDPR.

[23] Art. 6 para. 1 (c) GDPR.

[24] Art. 6 para. 1 (d) GDPR.

[25] Art. 6 para. 1 (e) GDPR.

[26] Art. 6 para. 1 (f) GDPR.

[27] Switzerland has, for example, enacted the Bundesgesetz über die Förderung von Sport und Bewegung (Sportförderungsgesetz, SpoFöG).

[28] Art. 6 para. 1 (f) GDPR.

[29] Art. 6 para. 1 (a) GDPR.

[30] Swiss Federal Tribunal, decision 133 III 235 et seqq., at para. 4.3.2.2.; Haas, Ulrich: The German Federal Court on Treacherous Ice – A final point in the Pechstein case, in: Müller, Christoph/Besson, Sébastien/Rigozzi, Antonio (ed.): New Developments in International Commercial Arbitration 2016, pp. 219 et seqq., at pp. 242 et seqq., regarding an essentially identical line of argumentation brought forward in the famous "Pechstein" case, concerning the "involuntary" conclusion of an arbitration agreement.

[31] Art. 4 para. 11 GDPR; see also GDPR, Recital 32.

[32] Schlarmann, Angela: Datenschutz beim Kampf gegen Doping, ZD 2016, pp. 572 et seqq., at p. 573; Neuendorf, Sabrina: Datenschutzrechtliche Konflikte im Anti-Doping-System, Bremen 2014, at pp. 109 et seqq., with further references. General legal literature on data protection law also tends to be quite strict when it comes to the "free" nature of consent. It is, for example, stated that the "voluntariness" of consent is the "defining requirement" of consent as a basis for data processing; Krohm, Niclas: Abschied vom Schriftformgebot der Einwilligung. Lösungsvorschläge und künftige Anforderungen, Zeitschrift für Datenschutz 2016, pp. 368 et seqq., at p. 369.

[33] GDPR, Recital 42.

[34] Legal literature accepts, for example, that the fact that data processing also serves the interests of a data subject can be taken into account when assessing the validity of consent declarations; cf. Wolff, Heinrich Amadeus/Brink, Stefan, Beck Online Kommentar, art. 7 GDPR at para. 50. It is also commonly accepted that the "free" nature of a consent declaration must be examined always on a case-by-case basis; Kühling, Jürgen/Martini, Mario: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 2016, pp. 448 et seqq., at p. 451; see also Wolff /Brink, art. 7 GDPR at para. 49, according to whom one shall assume that consent was not "freely" given only if this results from all circumstances of a specific case.

[35] By way of example only, the French data protection authority CNIL imposed, in January 2019, a fine in an amount of EUR 50,000,000.00 against GOOGLE LLC based on an alleged breach of the GDPR, for "lack of transparency, inadequate information and lack of valid consent regarding the ads personalization": see ‘The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC’, cnil.fr,21 Jan 2019, last accessed 30 May 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

COPYRIGHT NOTICE

This work was written for and first published on LawInSport.com (unless otherwise stated) and the copyright is owned by LawInSport Ltd. Permission to make digital or hard copies of this work (or part, or abstracts, of it) for personal use provided copies are not made or distributed for profit or commercial advantage, and provided that all copies bear this notice and full citation on the first page (which should include the URL, company name (LawInSport), article title, author name, date of the publication and date of use) of any copies made. Copyright for components of this work owned by parties other than LawInSport must be honoured.

Views 1976

Tags: Data | European Union | General Data Protection Regulation (GDPR) | Governance | Regulation | Switzerland

Tweet

RELATED ARTICLES

A practical guide to establishing the regulatory framework for a national esports federation

Why sports teams should avoid relying on consent to comply with GDPR

How the GDPR could impact the handling of sports disputes

Key information on the General Data Protection Regulation for the sports industry

ABOUT THE AUTHOR

DR. JAN KLEINER

Dr. Jan Kleiner is a Partner at Bär & Karrer, Switzerland

Full Profile

CAROL ETTER

Carol Etter is a Senior Associate at Cavaliero & Associates, Switzerland

Full Profile

LEAVE A COMMENT

Please login to leave a comment.

OFFICIAL PARTNERS

Contact Us | Terms and Conditions | Cookie Policy | Sitemap

Copyright © LawInSport Limited 2010 - 2018. These pages contain general information only. Nothing in these pages constitutes legal advice should consult a suitably qualified lawyer on any specific legal problem or matter. The information provided here was accurate as of the day posted; however, the law may have changed since that date. This information is not intended to be, and should not be used as, a substitute fo legal advice in any specific situation. LawInSport is not responsible for any actions taken or not taken on the basis of this information. Please the full terms and conditions on our website.