



**Navigating Sports and Data protection
and privacy;**
A Ugandan Perspective

*The worst thing about being famous is the invasion of your privacy
– Justin Timberlake.¹*

INTRODUCTION

Just like artists, sportsmen and women (athletes) operate in public spaces. From a professional point of view, showcasing sports talent is tailor-made for public consumption. Although the expectations of privacy for active athletes is reasonably lower, this does not blatantly extinguish the privacy rights of such sportsmen and women and neither does it extinguish the data protection obligation of the individuals and entities that collect, process, store or control the personal data of the athletes.

From a sports law point of view, the sports world is substantially and sensitively self-regulating. But this doesn't completely silence national, municipal and international laws that intertwine with sporting activities. This article analyzes how the sports world deals with data protection and privacy. Football (soccer) being one of the most regulated sports disciplines, several examples will be picked from this sport but not to the exclusion of others.

WHAT IS DATA PROTECTION/PERSONAL DATA?

Uganda's Data Protection and Privacy Act, 2019 (DPPA) defines data² as information processed by means of equipment operating automatically in response to instructions given for that purpose. Or information recorded with the intention that it should be processed or recorded as part of a relevant filing system or any information that forms part of an accessible record.

Personal data may be defined as any information relating to an identified or identifiable person referred that is recorded in any form.³ Such identification may be direct or indirect. Examples of such data include nationality, gender, body weight, height, blood group, age, educational level (this is an item often required in junior sports events), identification numbers (a good example is the National Identity Numbers NINs), mobile money numbers, etc. Courts of law have also found IP addresses to be personal data.⁴

The definition of personal data, is couched in a manner that is wide enough to cover both living and deceased persons as long as they are the data subjects in the circumstances.⁵ In sport, it is common to refer to data of the legends of the game. Examples of such data include the national football team that played in the 1978 African Cup of Nations finals, the Ugandan athletes that won

1 Summers, K.D., "Justin Timberlake: A Biography", 2010, ABC

2 Section 2.

3 Section 2, DPPA and Article 4, GDPR.

4 Patrick Breyer v Germany, Case 582/14, Court of Justice of the European Union (CJEU).

5 Muhangi, K., "Overview of Data Protection Regime in Uganda", 2019, available at <https://www.ktaadvocates.com/wp-content/uploads/2019/03/TMT-Overview-of-Data-Protection-in-Uganda-by-Kenneth-Muhangi.pdf> (Accessed on 3rd/08/2022).

the country her first medals in the Olympics and Commonwealth Games, etc. Many of these have since passed on, but their personal data is protected under our current legal regime.

The identified person or identifiable person is referred to as a data subject. This means that this legal regime only protects natural persons, not sports organizations such as the Uganda Rugby Union or sports clubs such as the UCU Lady Canons.

Personal data is confidential information that can only be obtained/delt with after obtaining prior consent of the data subject. The DPPA defines consent to be that which is freely given, specific, informed and unambiguous indication of the data subject's wish which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her

HISTORY OF DATA PROTECTION/PRIVACY

The right to privacy is a fundamental human right. The Universal Declaration of Human Rights (UDHR), 1948, provides that no person shall be subjected to arbitrary interference with his privacy, family, home or correspondences.⁶ The UDHR adds that everyone has the right to the protection of the law against such interference or attacks.⁷

The above provision is replicated under Article 17 of the International Covenant on Civil and Political Rights (ICCPR) of 1996. A similar provision is engraved under Article 27 (2) of the Constitution of the Republic of Uganda, 1995 (as amended).

The drafters of the international above international instruments might have foreseen personal data as one of such spaces into which the right to privacy extends but may not have envisioned the levels or way to which such data is being dealt with through automation, selling of data, data mining for machine learning, etc. Nonetheless, the drafters did make effort to demonstrate that the right to privacy easily extends to spaces such as private homes and correspondences.

The German Federal Constitutional Court in case 1 BvR 209, 269, 362, 420, 440, 484/83⁸ took judicial notice that the right to personal data protection was an extension of the right to privacy. The Bundeserfassungsgericht coined the right of informational self-determination, which maybe be defined as the desire of individuals to seek and enforce assurances that custodians of their personal data will comply with fair information practices.

Over time, the world has seen several successive phases of mechanization and automation of information, data collection, processing and storage. From the telegraph, to computers, to smart telephones, to supercomputers, etc. The rampant technological advancements continue to challenge the realization of the right to privacy in ways that few individuals can overcome alone.⁹ And the instruments assembled as early as 1948 do not have the clauses to tame modern-day practices. This is what has inspired several jurisdictions to tailor modern frameworks in the field of data protection and privacy.

6 Article 12

7 *ibid.*

8 1983 (the Census Case Judgement).

9 Seipp, D., "The Right To Privacy In American History", 1978, p. 102-13; see also Harv, L., "The Right to Privacy in Nineteenth Century America", Harvard Law Review, 1981, p. 94.

On the global stage, the maiden steps taken towards the regulation of data protection are traceable to the German state of Hesse which enacted the world's first Data Protection Act in 1970. But this was only at the state level and not a national law.¹⁰

The Swedish Data Act of 1973 is widely accepted as the first national legislative instrument on data protection.¹¹ The Act made it an offense for any person or entity to deal with personal data without a license.¹²

From an international perspective, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981 (European Convention of 1981) passed by the Council of Europe. Was the first international instrument on data protection. The Convention was operationalized by Directive 95/46/EEC. The directive made it incumbent on all EU Member States to protect and uphold the right to privacy for data subjects.

On the African Continent, on 27th June, 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection. As of the date of publication of this article, the Convention has 14 signatories, and 13 ratifications while 13 countries have deposited their instruments of ratification or accession.¹³

In Uganda, DPPA is the main legal instrument that governs data protection and privacy in Uganda. The Act prohibits the collection or processing of personal data in a manner that infringes on the privacy of a data subject.¹⁴

SPORTS AND DATA PROTECTION/PRIVACY

Before 2019, entities dealing with data in Uganda were de-facto self-regulating. Direction on data safeguarding was voluntary on based on international best practice or available policies for entities with international affiliations. Sports entities recognized by either the Uganda Olympic Committee or the National Council for Sports Council ought to have been in the latter category. This is pegged on the fact that such sports associations of federations have international affiliations that existed before 2019. For example, the Uganda Netball Federation is and was affiliated with the International Netball Federation much earlier than the DPPA came into force. This status logically inclined such sports bodies to observe the international best standards as demarcated by their bodies of international affiliation, but this was hardly the case.

SPORTS DATA PROTECTION LAWS

This segment is designed to give an insight on how some sports disciplines have taken extra steps to regulate data protection as an independent aspect of lex sport. The author elected to use football as the test discipline for this section this is because football has the most advanced data protection legal regime in lex sportive. The other sports disciplines

¹⁰ Olga Stepanova and Patricia Jechel, "The Privacy, Data Protection and Cybersecurity Law Review: Germany", 2021, available at [https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Overview,\(BDSG\)%20entered%20into%20force](https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Overview,(BDSG)%20entered%20into%20force). (Accessed on 18th/09/2022).

¹¹ GDPR Hub, Data Protection in Sweden, available at https://gdprhub.eu/Data_Protection_in_Sweden, (Accessed on 18th/09/2022).

¹² Ibid

¹³ African Union, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security And Personal Data Protection, available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (Accessed on 18th/09/2022).

¹⁴ Section 10.

either have less advanced or less detailed instruments or have no specific legal instrument regulating data protection.

In 2019, the Federation of International Football Association adopted the FIFA Data Protection Regulation (FDPR). The FDPR is applicable to FIFA and its member associations including the Federation of Uganda Football Association (FUFA) and all entities under the associations such as clubs. But the FDPR doesn't apply to associations or their clubs in circumstances where they collect or process personal data using their own infrastructure, for their own purposes, and in their own right if that FIFA or/and its other member associations have no connection to such transaction.¹⁵

Something noteworthy about the FDPR is that the Swiss Federal Act on Data Protection (FADP) is one of the applicable laws in this legal regime.¹⁶ This is a major diversion from the notorious international practice of using the European General Data Protection Regulations (GDPR) as the base instrument for data protection. This position is substantially due to the fact that Switzerland is not a member of the European Union yet Swiss law and Swiss Courts form the apex of the corpus of football law.

It is also pertinent to note that practice of some municipal sports associations or federations forming their own data protection regulations or policies. This is legally permissible, even for sports associations whose international affiliate bodies have no laid out instruments. But where the international affiliate body has an instrument, the local association has a duty to ensure that its local policies or regulations do not conflict with the instruments of its international affiliate body.

PILLARS OF DATA PROTECTION

6.1 Consent

It is unlawful to collect or deal with personal data of any nature unless such collection or dealing is done with the express consent of the data subject.¹⁷ The FDPR defines consent to be the freely given, specific, informed and unambiguous indication of the Data Subjects' wishes by which they (data subjects), by a statement or by a clear affirmation, signify agreement to the Processing of Personal Data relating to them (data subjects).

Where the data subject is a child, consent to collect or deal with such personal data must be sought from the parent or legal guardian prior to such collection or dealing.¹⁸ This is very important a practice for all sports academies and federations or entities that organize sports events for children.

There are two exceptions to the above rule that relate to the world of sport. Firstly, consent may be dispensed with if data is being collected in line with the performance of a contract that a data subject is a party to or in order to take steps to enter into a contract at the request of the data subject. For example, if an athlete clearly intends to join a club or has already joined a club, the club may collect personal data of such a player without first requiring his/her consent.¹⁹

¹⁵ FDPR, 2019, Regulation 3.

¹⁶ FDPR, 2019, Regulation, 2.

¹⁷ DPPA, 2019, Section 7.

¹⁸ DPPA, 2019, S.8.

¹⁹ DPPA, 2019, S. 7(2)(c).

The second exception is if the data is being collected or dealt with for medical purposes.²⁰ Accidents are a common occurrence on and off the pitch. In such circumstances, clubs or their medical teams do not need the express consent of the data subject before collecting or dealing with such data. For example, marathoners, motorsport riders and drivers openly disclose their blood groups before hitting the tracks. This is geared to words saving all precious time that may be definitive in saving lives of athletes. It is illogical to lose any time while seeking the consent of the data subject during medical emergencies.

6.2 Data Security

Sports entities that deal with data are mandated to ensure the integrity of personal data that they control or possess.²¹ To achieve this, sports organizations must deliberately design measures to safeguard data, prevent unauthorized damage, loss or unlawful access to such personal data. This achievable through designing data protection and security policy and implementing the same.

In case of any data breach, the data protection officers are mandated to report such breach to the relevant authorities and also detail actions taken to remedy the situation. The data collecting entity may then notify the data subject about the breach.

6.3 Rights of data subjects

Data subjects have a right to withdraw their consent. This enjoins with the rights to be forgotten. In such circumstances the processing of the data of the subject must be stopped. Such data cannot be retained for longer that what the data retention policy, that the subject agreed to indicates or as long as the law requires such data to be retained.

The data subject has a right to access their personal data. The data subject may also request that their data be or rectified corrected, or destroyed if such data is inaccurate or misleading.²²

Data subject should be informed about the collection of their personal data. Such information must capture the data being collected, the reason or purpose of collection, and any other relevant in respect to the collection.²³ This should b in a clear and simple language known to the data subject.

The data subjects have a right to lodge a complaint with the data protection officer (DPO) of the collecting entity or another regulatory entity such as the Personal Data Protection Office of Uganda. This creates an avenue through which a data subject can seek redress for any violation of their personal data.

The data subjects also have a right to demand that any decision that affects them is not taken basing solely on the automatic processing of their personal data.²⁴ And where a decision is made based solely on an automated process, that data subject has a right to be informed about the transaction.

20 DPPA, 2019, S. 7(2) (d).

21 DPPA, 2019, 20.

22 DPPA, 2019, s.16

23 FDPR, 2019, Regulation 5.

24 DPPA, 2019, Section 27.

6.4 Cross-border transfer of data

Sports entities collecting, processing, or storing personal data in Uganda may not transfer such data outside Uganda unless the country to which such data is transferred to with legal regimes that guarantee adequate levels of data protection²⁵ or where the data subject has consented to such transfer.²⁶ The FDPR also has a similar provision.²⁷

6.5 Data Retention

Sports entities need to clearly define for how long they intend to retain the personal data that they collect. These details ought to be availed in the entity's data retention policy. Data retention policies are crucial in the sports world. These enable tracing of a player's career which feeds into crucial calculations. For example, in football, such data is needed in calculating training and solidarity compensations.

The practice is that the maximum time for data retention is 10 years although the DPPA permits data retention for as long as necessary. But for sports record purposes, personal data is needed for historical purposes. For example, the sports world will still need to know the line-ups for the team that represented us in the AFCON finals of 1978 today and many years from now.

To be able to retain such vital data, sports entities have to make it clear how long they intend to retain such data and provided justification for the duration. Such data must be kept safely as highlighted in the data security segment.

CHILDREN AND DATA PROTECTION/PRIVACY

Averagely across the globe, a child is a person under the age of 18. This is the ceiling adopted by the UN Convention on the Rights of a Child.²⁸ For football, the FIFA Guardianship toolkit and policy define a child to be a person under the age of 18 years.²⁹

Children are vital pulley in the conveyor belt of any sports discipline. Several sports academies are hinged on child-athletes. Many sports associations or federations such the Uganda Swimming Federation directly tout their games in schools. A number of sport disciplines also have leagues or classes for children. For example, the Federation of Motorsport Clubs in Uganda (FMU) has a 50CC class of riders whose defending champion, the sensational Jamaira Makumbi is only seven years old.

Managing "kids" sports events or leagues involves collecting volumes of personal data. For example, Uganda organized the inaugural edition of CAF African Schools Championship National Qualifiers (July 2022). Schools register and gathered boys and girls at the Njeru technical center. The registration process involved collecting the names, dates of birth, copies of identification documents often bearing the photographs of the children, identification numbers, education level/class, et cetera. Such data is classified as personal data as envisaged under the DPPA.

25 DPPA, 2019, Section 19.

26 DPPR, Regulation 30.

27 FDPR, 2019, Regulation 7.

28 1989, Article 1.

29 Principal 2

Though the FIFA Data Protection Regulations do not pay specific attention for children, the FIFA guardianship toolkit mentions that every child has the right to take part in football in a safe and inclusive environment free from all forms of abuse, harassment and exploitation.

The inadequacy of international law on data protection for children creates ample room for the application of municipal laws on the subject. The DPPA provides that no one shall collect personal data of a child without the prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child. Personal data of a child may also be collected if the collection is necessary to comply with the law or for research or statistical purposes.³⁰

One would question whether sports regulations that require the registration of young athletes would qualify as a legal requirement as envisaged under the DPPA? The Interpretation Act of Uganda³¹ defines “written law” means the constitutional instruments, Acts, statutory instruments and any other legislative instruments having effect in Uganda.³² The Judicature Act Cap 13 adds Common Law, Custom and usage to the sources of law in Uganda.³³ The list of sources of law in Uganda doesn’t not accommodate private Sports Law instruments such as the FIBA Basketball Rules, 2022. These are private rules voluntarily made by entities and individuals that are willing to be bound by the same. Those such rules maybe a justification for collecting and processing personal data from children, they do not qualify as exceptions to the requirement of seeking the consent of parents or guardians before collecting personal data from children.

It is thus glaringly clear that even while dealing with personal data identifying children, data protection standards should not be lowered but heightened. Only necessary data should be collected and used specifically for the purpose it is collected for. But before such collection, a parent or guardian of the young data subject should consent to dealing with such data.

In addition to having data protection officers in sports data collecting, processing and storing sports institutions or communities, there is need to have guardianship or protection officers. These officers are more present in the football world where trained FIFA guardians ought to be designated for each footballing center. These are mandated to ensure that there is a safe environment for children to play without being abused or exploited. These responsibilities inter alia include data protection.

The growth of women’s football also presents a new frontier in the fight for safe playing spaces for all. Several young female athletes have reported receiving unsolicited phone calls from strangers churning out obnoxious language that could easily be classified as sexual harassment. Such unfortunate incidents are a testament to the unlawful disclosure of personal data, to wit, mobile telephone numbers of young athletes. Something that ought to be worth the attention of sports DPOs and guardianship officers.

30 Section 8.

31 Cap 3.

32 Section 2.

33 Section 14.

REGISTRATION WITH THE PERSONAL DATA PROTECTION OFFICE

Sports entities that deal with personal data in Uganda are mandated to register with the Personal Data Protection Office (PDPO). Currently, the records of the PDPO indicate that no sports entity has registered with the PDPO. This is a testament to the poor data protection levels in Ugandan sport. This status quo also indicates that all national sports associations, federations, sports clubs, sports leagues etc, are operating in breach of the data protection legal regime in the country.

PROHIBITION OF COLLECTION OF SPECIAL PERSONAL DATA

The DPPA, prohibits the collection of certain categories of personal data referred to as “special personal data”.³⁴ This includes data that relates to the religious beliefs, political opinion, sexual life, financial information, health status or medical records of a data subject.

The FDPR adds these categories of personal data to the list; philosophical beliefs, trade union membership, genetic data, biometric data, and data concerning a natural person’s sex life or sexual orientation.³⁵

Some of this data such as revealing gender, financial information to make payments, medical data, especially during the transfer of players, etc, is often required by sports entities and associations. Such collection is permissible if required by law, when freely given by the data subject, or when the collection is for legitimate sports activities. The FDPR requires that if collected, such data should be afforded special protection.

Entities and sports associations that wish to collect such data must take deliberate measures to ensure that the data subjects’ consent to collecting such data is not a product of undue influence or coercion by the data collectors.

CONCLUSION

In his 1991 article titled “On the Utility of Constitutional Rights to Privacy and Data Protection”³⁶ David H. Flaherty opined as follows;

“Privacy is like freedom: we do not recognize its importance until it is taken away..... it is a personal right that we assume we have yet take for granted-until something or someone infringes on it privacy, like freedom, is difficult to define except in the negative.”

Article 1 of the UDHR starts by affirming that all humans are born FREE. As David H. Flaherty puts it, the right to privacy is a crucial pillar to the realization of human freedoms and the sports world is no exception to this position.

³⁴ Section 9.

³⁵ Regulation 4(2).

³⁶ David H. Flaherty, “On the Utility of Constitutional Rights to Privacy and Data Protection”, Case Western Reserve Law Review, p. 1, 1991.






**TIMOTHY
KAJJA**

ASSOCIATE
TMT&IP

Sports entities should work towards the observation of internationally acceptable data protection and privacy standards. This involves taking steps such as having modern data protection and privacy policies, data retention, data security policies, and related policies. Sports entities should also register with authorities responsible for personal data protection in the jurisdictions in which they operate such as the PDPO in Uganda.

By Timothy Kajja.

Contact us

 3rd Floor, Plot 4, Hannington Road
P.O. Box 37366, Kampala, Uganda.
 +256 414 530 114 | +256 200 906 545
Fax: +256 414 531 078
 partners@ktaadvocates.com