

DATA PROTECTION AND PRIVACY ISSUES IN SPORTS ADMINISTRATION IN NIGERIA

Prof. Timothy Ifedayo Akomolede¹ and Dr Bernard Oluwafemi Jemilohun²

¹(Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria)

²(Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria)

Abstract: *Sports administration in Nigeria is both a public and a private issue and as both levels of government are involved, a lot of records and personal information is involved. It is common knowledge that the advent of information communication technology has made information creation and dissemination much easier and faster than before and this calls for effective regimes for the protection of personal information. This article examines the evolution of sports administration in Nigeria and the place of informational privacy and data protection. It points out that though the field of sports law in Nigeria is a developing field of law, there is the need for the parties involved to ensure that risks are minimised while the integrity of sports is preserved. Since sports practitioners and administrators collate and process data from time to time, they must recognise the limits that are imposed on the use, transfer and exchange of such data. The article draws lessons from other jurisdictions and points out though there are Guidelines for data protection in Nigeria, she does not yet have an effective data protection regime and thus much needs to be done to protect personal information in the field of sports as well as other fields.*

Keywords: Personal Information, Sports Administration, Data Protection

Research Area: Privacy Law

Paper Type: Research Paper

1. INTRODUCTION

The need to protect personal data has moved from simple private interests to matters of global and international concern. (Taubman, 2009) Earlier on, it was a matter that few nations had a real interest in but as the European Union (ECHR Art 8) took a deeper and more detailed interest in the issue, it began to spread across global frontiers. It did not stop there, issues of personal information protection also progressed from just a concern of governmental abuse of personal information of the citizens to the need for citizens to protect each other from the possibilities of personal information abuse by each other.

The field of sports administration in Nigeria is a matter that occupies a major place in government. The Nigerian nation is one of sports lovers and one may fairly say that sport is one of the major unifiers of the diverse ethnic groups that make up the nation. Sports administration in Nigeria is headed by a Minister of the Federal Government who is appointed by the president after a screening by the national assembly. Though the Constitution does not explicitly lay down special requirements for an appointee to the office of the Minister of Sports, there are expectations that such a person should have good oversight knowledge of sports administration issues in the country.

The need for laws to regulate human interactions in society, warns against deviant behaviour and punish criminality has been long recognised. The field of sports administration

has not been one without laws in Nigeria but as pointed out by Omuojine (2013) there is not only the absence of a statutorily recognized body with a primary duty of sports development, there is the absence of mechanisms for the resolution of sports disputes in Nigeria. The need for a clear understanding of the possibilities of disputes and other matters of legal infringement in sports matters in Nigeria cannot be under-estimated.

Traditionally, privacy as a right was first given judicial recognition in the case of *Prince Albert v Strange* (1849) where the court held that the common law rule prohibited not merely the reproduction of the etchings which the plaintiff and Queen Victoria had made for their own pleasure, but also the “the publishing (at least by printing or writing), though not by copy or resemblance, a description of them, whether more or less limited or summary, whether in the form of a catalogue or otherwise”.

Warren & Brandeis (1890) defined the protection of the private realm as the foundation of individual freedom in the modern age. In their view, because of the increasing capacity of the government, the press and other agencies and institutions to invade aspects of personal activities that were previously inaccessible, the law must respond to technological change. And with the technological innovativeness that the computer’s invention has brought upon humanity, issues hitherto unthought-of are emerging and thus every player on the field need to be aware of the risks and possibilities of violations and infringement of other people’s rights that are possible by technology.

2. METHODOLOGY

There are three broad types of research methodology applicable to this type of writing: the doctrinal, the comparative and the non-doctrinal. This article adopted the doctrinal approach as it examined the provisions in the law books. The research made use of both primary and secondary sources of information. The primary sources include statutes and instruments like the Constitution of the Federal Republic of Nigeria, 1999, the NITDA Act, 2007, the European Union Data Directive, and also judicial decisions from courts. The secondary sources include textbooks, journals, articles, materials from the Internet including blogs and posts on websites, magazines, newspapers etc.

3. SPORTS ADMINISTRATION IN NIGERIA

The administration of sports in Nigeria is both a public enterprise and a private one. The governments at both the federal and the state level are heavily involved in the administration of sports. There are also private interests involved in sports administration. One cannot escape the fact that many persons who are involved in sports do so not just for physical fitness or leisure but for career and also investment purposes. Sport has amassed a huge commercial significance over the years both nationally and globally.

At the public level, sports is administered at the State level through Sports Councils and at the National level through the National Sports Commission. One may say the historical evolution of the National Sports Commission started with the promulgation of Decree 34 of 1971 which formalized and legalized the National Sports Commission (NSC) as the apex Federal Government agency to control, regulate and organize sports in Nigeria. This went on

till 1975 when the National Sports Commission was elevated to the status of a Ministry with a Cabinet Minister.

However, the promulgation of Decree 7 of 1991 saw the re-emergence of the National Sports Commission as a parastatal under the Ministry of Youth and Sports. Further, in 1995, the National Sports Commission was scrapped and the administration of sports was once again transferred to the Ministry. In December 2006, the Olusegun Obasanjo administration reverted the then Federal Ministry of Sports and Social Development (FMSSD) to the National Sports Commission. Prior to this development, the then Ministry had recognized 34 National Sports Federations.

The oscillation of the administration of sports between the Federal Ministry of Sports and the National Sports Commission was a major factor militating against the desired growth and development of Sports in Nigeria. Sports management structure suffered some setbacks as a result of poor implementation or outright non-implementation of the 1989 National Sports Policy, which was Nigeria's first Sports Policy. (National Sports Policy of Nigeria, 2009)

Sports administration and practice in Nigeria today have taken a new and great dimension, thereby becoming a big commercial venture and employer of labour (National Sports Policy of Nigeria, 2009). This has also led to the emergence of a new area of law known as Sports and Recreation Law which focuses on legal issues pertaining to the sports industry. It is not a separate body of law but refers to the target industry addressing the few but unique legal issues faced by professional sports colleagues, administrators and club owners and other stakeholders within the sports industry.

4. THE PLACE OF INFORMATIONAL PRIVACY AND DATA PROTECTION

With the advent of the computer comes an explosive use of information communication technology. It is common knowledge today that the computer has permeated every sphere of human life and many people who were born in the last 20 years cannot imagine a world without computers. The emergence of the internet as a global information highway linking millions of people via different machines and methods has literally reduced the entire world into a global village. Much as this development has brought progress and prosperity to mankind, human beings have also learnt to use the same instruments for all manner of anti-society behaviour.

The computer and the internet have become the greatest technologies for information dissemination; (United Nations, 1994) there is the recognition for strong legal regimes or frameworks to govern data in the information communication technology world. This would have been easy if the internet were domiciled within one territory. The fact that the internet is not just one huge machine but the interconnectivity of millions of computers connected via telephone lines, fibre optics, satellite, vertical masts, very small aperture terminal (VSAT) etc. make legal governance of the internet very difficult. And the fact that laws have territorial limitations and conventions that are only binding on countries which accede to them have not made things easier.

Yet, the reality on ground now is that organizations, agencies and institutions store a large amount of information in electronic format and due to the possibility of networking, organizations that run in multi set-up systems (including sports clubs and sports administrators) devise methods and means of keeping their information on several servers or computers in different places all linked up on the internet. Granted that the operators of these systems and other staff of such organizations are committed to integrity and data security, what happens where an employee is ‘improperly’ relieved of his job and in his grief, decides to harm the club or the sports commission? Or where an outsider with computer intelligence and criminal motivation has access to such information or hacks the system where such information is stored? The extent of damage is better imagined than experienced.

This right to informational privacy and data protection is more evident in the light of the possibilities in cyberspace. With the ease of transfer of files on the web and the possibilities of extra-territorial access to information without borders, nobody should assume that his profile on the web is safe merely because of a set of passwords or other encryption techniques that he has employed or deployed. The world has become a global colony and thus personalities in the online world are ‘closer’ than in the real (offline) world. Since online transactions are actually meant to save one from the stress of physical presence and the hazards involved therein, there is the necessity to ensure that harms resulting from violations of informational privacy are prevented.

Since sports practitioners and administrators from time to time collate and process data, there have been new technologies for data acquisition and processing in the sports world. But while processing of personal data is allowed to a reasonable level, there are also limits that the law imposes to the use, transfer and exchange of such data. The administration of sports in Nigeria involves some risks. Granted that the law of sports in Nigeria is a developing area of law, there is the need for the different parties involved to ensure that risks are minimised while the integrity of sports is preserved. But managing risks is not just about health and safety and insurance, it is about data protection too. Parties at various levels in the sports arena are subjects of data protection and informational privacy.

Virtually every nation on the globe has found it necessary to not only legislate for personal informational privacy or data protection, but several have also established specialised agencies to enforce the legislation and ensure compliance with the different categories of people and organisations processing the personal data of private persons.

5. PRIVACY AND DATA PROTECTION ISSUES IN SPORTS

In the past concerns about privacy within the sports world would focus around issues such as the use of open locker rooms and general bathrooms without much regards for the individual dignity and identity of the players or athletes. (*Vernonia School District 47J v. Acton*, 1995). The Supreme Court of the United States noted that there is an element of communal undress inherent in athletic participation. Though this description by the Court of participation in athletic programmes sounds almost militaristic, yet regimentation well beyond the side-lines or the walls of the gym is accepted as a routine feature of sports, and bodily privacy is compromised. (McChrystal 2001) Later developments brought concerns for matters like drug testing for athletes, and the appropriateness or otherwise of making such

results public. Then the issue of police searches of spectators at sports events has also been considered as matters of privacy.

But technology has made privacy invasion much easier and the possibilities of damage to the dignity and personal honour of individuals may not be easily quantified. On the other hand, such may result in grave financial liabilities to club owners, sports administrators and others. An example is the United States case of *Does v Franco Productions* (2000) where 28 young men sued Franco Productions and others for compensatory and punitive damages based upon invasion of privacy, unlawful use of the plaintiffs' images for monetary gain, and mail and wire fraud under the federal Racketeer Influenced and Corrupt Organizations Act for secretly videotaping in locker rooms, restroom and shows at Northwestern University, USA in 1995.

The secret videotapes were sold on the Internet and advertised as "hot young dudes." The tapes carried names like "Straight Off the Mat" and "Voyeur Time" when they first came to light in April 1999, and they depicted hundreds of young athletes in various degrees of nudity.

The court gave judgment in favour of Plaintiff in the amount of \$500 million. Each identified athlete was awarded \$1 million in compensatory damages and \$10 million in punitive damages by the Court. The court also ordered the defendants to stop making and selling the tape and to surrender the videotapes. This is a clear example of personal privacy violation and the court rose to the challenge of not just punishing same but fairly compensating the victims. It does not require the gift of soothsaying to know that the times will come when violations of personal data will likely attract similar sanctions.

Within the ambit of public sports administration in Nigeria, it may be easier to think that the protection of the personal information of sports personalities is not a potential problem or a serious issue. But with the participation of private interests in sports especially in matters of sponsorship, branding, broadcasting rights and outright ownership of clubs and with so much data in the hands of private organisations and commercial enterprises, certain issues need to be addressed. ("Policies and Procedures", 2018) Globally, a combination of several key political, commercial and technological issues has resulted in the elevation of private enterprise above national governments as the largest potential threat to personal data privacy. According to Charlesworth, (2000) some of these are:

- Private enterprises are better at data processing.
- Private enterprises have more motivation to push the envelope of acceptable personal data use.
- Private enterprises are subject to limited public control.
- Private enterprises have benefitted from the free market and deregulation ethos of recent years.
- Private enterprises have been given a larger role to play in international organizations.
- Private enterprises are often able to relocate internationally.

- Private enterprises dealing primarily in data can relocate internationally more easily.

It is also important to note that there is an emerging classification of personal information that is known as sensitive data and this relates to things like passwords; financial information such as bank account or credit card or debit card or other payment instrument details; physical, psychological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above received by the body corporate for the provision of services; or any information relating to the foregoing that is received, stored, or processed by the body corporate under lawful contract or otherwise. (India. Data Privacy Rules)

Thus club owners, sports commissions and other sports administrators, players and athletes have definite duties not to violate the private personal information of others either by sharing them without authorisation or however transferring them without adequate protection under the extant laws and regulations.

From analytics to big data to wearable technology, much information about sportsmen and women are collected almost on a daily basis. With the relocation and transfer of sportsmen and sportswomen from one club to another or even national territories, information gathering may not be curtailed but the need for protection is more evident. This places some sort of responsibility for adequate preservation of the integrity of personal information. Thus it will be largely risky for sports administrators and club owners not to know the importance of the data they are gathering or for them to think data and personal information gathered concerning sportsmen and women may be marketed against their wish or negatively used against them by unwarranted and illegal exposure to the public.

A major privacy issue with respect to sports personalities is the issue of health records. Sports clubs are in a unique position in an employment context as they are likely to regularly process health information relating to their players, including medical histories, medication, allergies, injuries and potentially medical information which may or may not be specific to the sport itself. (Russell, 2018) From the time of engagement and contract formation, clubs and national sports administrators may by the terms of the contract demand that sportsmen disclose certain information with regards to their health status. This may be important in helping sports business reduce or determine their liabilities in the future. But such disclosure is one of a very serious matter. Whether the sportsman or athlete is retained or not on account of the health status, such information must not be passed to another person or organisation except reasonable safeguards are in place and the law is not violated.

6. THE LEGAL REGIME FOR INFORMATIONAL PRIVACY AND DATA PROTECTION IN NIGERIA

The concept of informational privacy or personal data protection in Nigeria is still an emerging issue in Nigeria. Though there is no single legislation directed specifically towards informational privacy or data protection in Nigeria, there is a provision in the 1999 Constitution of the Federal Republic of Nigeria which guarantees and protects the privacy of the citizens. The Constitution provides in S. 37 as follows: “The privacy of citizens, their

homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.” In the view of Akinsuyi, (2010) this Constitutional provision should be enough impetus to propel the law-making authorities in Nigeria to enact a standard informational privacy or data protection legislation. But till date, this has not been the case.

The closest that Nigeria presently has as Data Protection legislation that regulates the processing of personal data or affords any protection to informational privacy is the Guidelines for Data Protection that was released by the Nigeria Information Technology Development Agency (NITDA). The guidelines are purportedly issued pursuant to Sections 6, 17 and 18 of the NITDA Act (2007) and a breach of the guidelines is deemed to be a breach of the Act. The guidelines further provide that it shall be subject to periodic review by the agency while it permits additional data protection and security guidelines to be developed and used at organisation discretion in accordance with the rules.

7. THE NITDA DRAFT GUIDELINES FOR DATA PROTECTION

The preamble to the National Information Technology Development Agency Draft Guidelines on Data Protection alludes to the mandate of the NITDA as given by the NITDA Act 2007 to develop information technology in Nigeria through regulatory policies, guidelines, standards, and incentives. It states further that part of the mandate is to ensure the safety and protection of the Nigerian citizen’s personally identifiable information otherwise known as personal data and successful implementation of guidelines on data protection.

The NITDA Draft Guidelines on Data Protection is divided into three main sections. Section one covers matters like the preamble, the authority on which the guidelines are based, the scope and application of the guidelines, the purpose and definition of terms. Presented in Section two are guidelines for data protection, data processing, data access and data security officers. Areas covered in Section three include principles of data protection which are in *pari materia* with the data protection principles enunciated in the European Union Data Protection Directive and which have been incorporated into the various data protection laws of other nations that have legislated on the same.

It is worth noting that the Draft Guidelines specifically state that its purpose is to prescribe guidelines for all organizations or persons that control, collect, store and process personal data of Nigeria residents within and outside Nigeria for the protection of Personal Data or Object Identifiable Information (OII) and to prescribe minimum data protection requirements for the collection, storage, processing, management, operation and technical controls for personal information.

In delimiting its own scope, the guidelines shall cover the processing of personal data whether by the automatic system or by other means where they form part of a filing system, it will also cover data controllers or processors operating within Nigeria or processors outside Nigeria if they process personal data of Nigerian residents. Though the guidelines stipulate that it shall apply to all data processors whether, in the public or private sector, it does not cover the processing of personal data, processing operations concerning public security, defense, national security and the activities of the nation in areas of criminal law.

The Draft Guidelines are classed into Guidelines for Data Collection, Guidelines for Data Processing, Guidelines for Data Access, Guidelines for Data Security Officers and lastly, Principles of the Data Protection Guidelines which are in every respect an adaptation of the following eight core data protection principles: (Directive 94/46/EC)

- i. Personal data must be processed fairly and lawfully
- ii. Personal data shall only be used in accordance with the purposes for which it was collected
- iii. Personal Data must be adequate, relevant and not excessive
- iv. Personal data must be accurate and where necessary kept up to date
- v. Personal data must be kept for no longer than is necessary
- vi. Personal data must be processed in accordance with the rights of the data subjects
- vii. Appropriate technical and organizational measures must be established to protect data
- viii. Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection.

The guidelines (in Section 2.1.1) places the responsibility for the protection of the privacy of natural persons on Data controllers who are natural or legal persons, public authority, agency or any other body which alone or jointly with others determine the purposes or means of processing personal data. The data controllers are to secure this privacy in accordance with the guidelines and the provisions and prescriptions of Section 5, Part 1 and Part 2 of the National Information Systems and Network Security Standards and Guidelines.

Secondly, the guidelines expressly prohibit the collection of personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of personal data concerning health or sex life except on some conditions: the data subject has consented explicitly to the collection and processing; or the collection and processing are necessary for the purposes of carrying out the obligations and specific function of the controller in the field of employment; or collection and processing is necessary to protect the vital interests of the data subject or another where the data subject is incapable of giving consent; or collection and processing is carried out in the course of its legitimate activities with appropriate guarantees by a relevant association or other non-profit-seeking body and that the processing relates only to members of the body; or the collection and processing relates to data which are made public by the data subject or is necessary for legal matters

Thirdly, where the data was not obtained from the data subject, the controller must at the time of recording the personal data provide the data subject with information about the identity of the controller, the purposes of the processing, further information such as the categories of data concerned, the recipients of such data and the mechanism for access to and rectification of the data concerning him.

The fourth guideline deals with the transfer of personal data which are undergoing processing (or which are intended to be processed after transfer) to another country. This is only permitted where the country in question ensures an adequate level of protection.

The fifth provision under these guidelines gives data controllers a moratorium of 12 months from the date of adoption of these guidelines, within which to bring directives and administrative provisions necessary to comply with them. The import of this is that companies processing data are not under any serious legal duty to conform or comply with the provisions of the guidelines until the same is adopted.

The last guideline for data collection requires organizations to implement effective privacy policies and procedures and state those policies both online and offline in order to ensure that Nigerian people understand and have confidence in the proper use and safety of personal information. As has been pointed out earlier, these are just guidelines. How effective these will be in a country like Nigeria with a low literacy level especially in the area of information communication technology is left to time.

One may observe that Nigeria is not as developed as the American society where people can be expected to ensure that their personal information is not abused. This is one more reason why the NITDA Draft Guidelines may not be sufficient as a data protection instrument. As developed as the United States is, there have been arguments as pointed out elsewhere by Jemilohun & Akomolede, (2015) that the absence of a data protection authority similar to the European model is not good enough. A developing economy like Nigeria needs to invest in very strong institutions to ensure that the expectations of the law especially in new areas like this are met.

8. LESSONS ON DATA PROTECTION WITHIN THE SPORTS SECTOR IN UK

The United Kingdom is a leader in the field of data protection. As a member of the European Community, it was mandatory to comply with the EU Data Protection Directive and also make legislation for data protection within her territory. The UK Data Protection Act of 1998 was the result then but same has been replaced with the General Data Protection Regulation (2016) which sets out to give far greater powers to data subjects and introduces substantially tougher fines for non-compliance. However, since the new enactment will apply to personal data violations and incidents occurring after 25 May 2018, it remains important that data processors and similar agencies are familiar with the provisions of the 1998 Act.

The new Regulations pointed special attention to matters like “special category” and “sensitive personal data” which attract heightened protection and these are data revealing a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life, sexual orientation or trade union membership.

Within the United Kingdom, (“Policies and Procedures”, 2018) there are agencies and bodies working with sports clubs and alliances to help the sector become compliant by creating a suite of templates such as privacy policies, data usage statements and template forms. The templates will be supported by guidance notes and advice summaries to help clubs and organizations use them correctly and adapt them to their individual needs.

9. THE CHALLENGES OF DATA PROTECTION TO SPORTS ADMINISTRATION IN NIGERIA

There are many issues affecting informational privacy and data protection in Nigeria generally, and the field of sports administration is no exception to this. Jemilohun (2015) observes that despite the constitutional guarantee in S. 37 of the 1999 Constitution and the NITDA Data Protection Guidelines, the major problems noticeable with data protection in the Nigerian cyberspace include:

- (i) lack of comprehensive laws protecting the privacy of citizens yet the Constitution guarantees that the privacy of citizens shall be protected;
- (ii) absence of a legal framework that deals with the ownership of private and sensitive information and data;
- (iii) lack of certain and definite procedures for creating, processing, transmitting and storing of sensitive information and data;
- (iv) lack of a classification of information as public information, private information and sensitive information;
- (v) lack of provisions that stipulate the standards for data quality, proportionality and data transparency; and
- (vi) absence of a clear and definite legal framework or legislation that deals with cross-country flow of information.

The outflow of the foregoing is that sportsmen and women in Nigeria do not have clearly defined rights over their personal information and where a perceived right is breached, remedies may not be adequate. For example, there are no specific legislation that prohibit the indiscriminate transfer of the personal information of a player from one club to another. A club may erroneously assume that information about players in its custody is absolutely it's own whereas the player inherently has privacy rights that ordinarily should not be breached.

Added to the foregoing is the absence of any institutional framework or any definite agency to ensure compliance with any regulation made for data protection for sportsmen. The lack of a specific agency to enforce compliance with data protection regulation is a major reason why breaches and violations may go unpunished and abuse may continue.

As it is known generally, regulations are not legislation and thus do not create enforceable laws in the courts. Regulations at best stipulate penalties payable where violation takes place and much as this may fill up the coffers of the nation, they do not in any way assuage the loss of the parties whose rights have been breached or are about to be breached. English courts earlier developed a means by which the breach of confidential information could be prevented, and thus there was a tort of misuse of private information. (Campbell v. MGN Ltd 2004). Under the action, a claimant must first establish a 'reasonable expectation of privacy' in relation to the information that is threatened with disclosure (Murray v. Express Newspapers 2008). If found, the next question is whether there is a public interest justification for the disclosure and whether an injunction against disclosure would both be necessary and proportionate. Sometimes, it may not be too easy to determine these issues.

But in countries with an effective legal regime for data protection, controls are placed on the processing of personal data, whether the information is private or not and before abuse arises. Thus it is not about competing interests between the public and private persons but that private personal information is deserving of protection

Thus a footballer whose sexual orientation, for example, is carelessly revealed by the officials of his club may not have any compensatory remedy in Nigeria which is similar to the remedies or compensations his colleagues in the United Kingdom and other soccer-loving nations may deserve. The only route for such a person to obtain legal redress may be through the tort of misuse of private information. How easy this will be for the aggrieved sportsman is a matter of guesswork.

10. CONCLUSION

It can be seen that the advent of technology has brought upon mankind more possibilities of a privacy invasion that was conceived in the past. The possibilities that the Internet has brought upon us are more than was envisaged at the outset of the computer age. This has necessitated nations and regional bodies enacting adequate legislation to place duties and burdens on the shoulders of data processors and sports administrators owe their sportsmen and sportswomen the obligation to ensure that their privacy is protected.

Nigerian lawmakers should respond to the changes in the technological environment and like lawmakers in other civilised climes make adequate laws that secure the interests of the private citizen against violations encouraged by technology. Informational privacy or personal data is to be processed and handled with care and concern for the objects of the data. It is important that sports administrators know the importance of the personal data or sensitive personal information of sportsmen and women who have contractual obligations with them or whose data they are involved in processing.

11. IMPLICATIONS FOR NIGERIAN SPORTS POLICY

It goes without saying that sports policies in Nigeria must take into cognizance the need to provide for the protection of the personal data of sportsmen and women. Policy makers and administrators must become aware of legal issues and rights of the various parties to the sporting contracts. This is necessary to minimise liabilities that may be incurred due to the abuse of personal information of sportsmen.

Nigerian sports administrators must put in place appropriate measures to ensure that officers of government or club owners comply with the guidelines for data protection while entering, processing or transferring personal information of players. Sports policies must of necessity involve specific guidelines as to what manner of information may be collected from sportsmen and women and stipulate the need to make the persons whose information are to be processed know what the information will be used for.

Finally, sports policies should mandate sports administrators and sports club owners to observe global best practices in protecting personal information and ensuring the preservation of human dignity even where a sportsman is no longer in the employment of a government or a club.

REFERENCES

Cases

- Campbell v. MGN Ltd* [2004] UKHL 22 at para 14
- Does v Franco Productions* No. 99 C 7885, 2000 U.S. Dist. LEXIS 8645, at *11 (N.D. Ill. June 8, 2000) (citing 47 U.S.C. § 230(c)(1) (2000)).
- Murray v. Express Newspapers* [2008] EWCA Civ 446
- Prince Albert v Strange* 1 McN. & G. 23 (1849)
- Vernonia School District 47J v. Acton* 515 U.S. 646 (1995)

Articles

- Akinsuyi, F. F. (2010) Data Protection Legislation for Nigeria: The Time is Now! Available at <http://www.Nigerianmuse.com>
- Charlesworth, A., (2000) Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual in Edwards, L. & Waelde, C., (eds.) *Law & the Internet, A Framework for Electronic Commerce* (Oxford, Hart Publishing)
- European Union Data Directive (Directive 94/46/EC of the European Parliament and of the Council of and also Part 1 to the United Kingdom Data Protection Act, 1988
- Jemilohun, B. O. & Akomolede, T. I. (2015) Regulations or Legislation for data Protection in Nigeria? A Call for a Clear Legislative Framework. *Global Journal of Politics and Law Research*, Vol. 3, No. 4
- Jemilohun, B. O. (2015) *An Appraisal of the Legal Framework for Data Protection in Cyberspace in Nigeria* (Unpublished doctoral thesis). Ekiti State University, Ado-Ekiti
- McChrystal, M. K. Privacy in Sports: Recent Developments in the Federal Courts, 12 Marq. Sports L. Rev. 397 (2001) Available at <http://scholarship.law.marquette.edu/sportslaw/vol12/iss1/13>
- Omuojine, K. (2013) The Legal Framework for Sports Development in Nigeria. Africa Sports Law and Business Bulletin 1 available at www.africansportslawjournal.com/Bulletin%201_2013_Omuojine.pdf.
- Policies and Procedures, Data Protection Policy and Changes to GDPR available at www.sportenglandclubmatters.com/club-planning/governance/policies-procedure/data-protection-policy
- Russell, K. (2018) Why Sports Teams Should Avoid Relying on Consent to Comply with GDPR available at <https://www.lawinsport.com/topics/articles/item/why-sports-teams-should-avoid-relying-on-consent-to-comply-with-gdpr>
- Taubman, A. (2009) International Governance and the Internet in Edwards, L. & Waelde, C., (eds.) *Law and the Internet* 3rd ed. (pp. 3-44) Hart Publishing, Oxford
- United Nations Manual on the Prevention & Control of Computer-Related Crime. Retrieved from <http://www.uncjin.org.80/Documents/irpc4344.pdf>
- Warren, S D., & Brandeis, L. D., (1890) The Right to Privacy, 4 *Harv. L. Rev.* 193