ENTERTAINMENT AND SPORTS LAW JOURNAL

Flanagan, CA, et al. 2022. Stats Entertainment: The Legal and Regulatory Issues Arising from the Data Analytics Movement in Association Football. Part Two: Data Privacy, the Broader Legal Context, and Conclusions on the Legal Aspects of Data Analytics in Football. *Entertainment and Sports Law Journal,* 20: 1, pp. 1–16. DOI: https://doi.org/10.16997/eslj.1082

REVIEW

Stats Entertainment: The Legal and Regulatory Issues Arising from the Data Analytics Movement in Association Football. Part Two: Data Privacy, the Broader Legal Context, and Conclusions on the Legal Aspects of Data Analytics in Football

Christopher A. Flanagan
Solicitor, UK
ChristopherAFlanagan@gmail.com

Data analytics has become a critical part of professional football. It brings with it a number of challenging legal questions, brought into sharper focus by the reported 'Project Red Card' legal action, in which the legality of the systematised use of player performance data has been called into question. Focussing on the position in English law, this two-part article takes a holistic approach to assessing the legal issues presented by the data analytics movement.

Part One set out contextual information on the development of data analytics in football before examining whether the data produced in football are capable of ownership, either in raw format or after manipulation, taking into account the nature of property and intangible assets, relevant intellectual property laws, and non-IP protections.

Part Two goes on to consider the position in respect of data protection law (including FIFA's Data Protection Regulations) before taking into account some broader legal issues, such as the application of competition law and the regulation of artificial intelligence.

The conclusions of Part One and Part Two together are that the intellectual property rights position is broadly positive for data analysts, with legal protections capable of application in many circumstances. However, data protection law presents a more complicated problem, with a number of challenging compliance obligations for the analytics community, albeit with scope to exploit player performance data where those obligations are met.

Keywords: Analytics; Football; Data Protection; GDPR; Artificial Intelligence; Competition

1. Data privacy law

1.1. Background

The revolution in data analytics described in Part One of this article happened in tandem with a considerable development in data privacy law in the EU, which contains some of football's most commercially and technologically developed markets. Where intellectual property law provides little in the way of empowerment to the players on whom the data analytics industry is built, the data protection law landscape is quite different, conferring rights upon players and adding considerable compliance burden to data analysts. Part Two will analyse the prevailing data privacy landscape and its considerable impact on analytics in football.

At a sports governing body (SGB) level, there has also been some movement to recognise the complexities of data usage within the modern game in the form of the Fédération Internationale de Football Association (FIFA) Data Protection Regulations, introduced in October 2019.[1] The scope and impact of the FIFA Data Protection Regulations is considered in section 1.10.

Section 2 of Part Two will go on to examine at a high level some of the other legal issues faced by the use of data in football, such as competition law and the forthcoming regulation of artificial intelligence (AI) at the EU level.

Data privacy is deeply enshrined in EU and UK law. The right to 'protection of personal data' is found at Article 8 of the EU Charter of Fundamental Rights, which was given the force of law by the Treaty of Lisbon (albeit subject to a UK opt out). The principal legal instrument for data protection in the EU is the General Data Protection Regulation[2]

(GDPR). As an EU regulation pre-Brexit, the GDPR had direct effect in UK law (subject to certain limited derogations), although certain aspects of the GDPR required domestic implementation akin to an EU Directive (Lloyd, 2020: 37) and the GDPR was thus further enshrined in domestic law in the form of the Data Protection Act 2018 (the DPA 2018). These instruments replaced the Data Protection Directive (Directive 95/46/EC) and the Data Protection Act 1998 (each now repealed) in the EU and UK, respectively.

The GDPR 'aimed to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement' (Kuschewsky, 2016, Chapter 1.1), significantly modernising the data protection framework by introducing a number of changes to the existing data protection framework, including an increase to the severity of the available sanctions, a broadening of the scope of personal data caught, an augmentation of data subject rights, a widening of territorial scope, development of the requirements for processing and for transferring data, changes to the respective responsibilities of 'controllers' and 'processors' (terms of art in data protection law), and more.

In general, EU and UK data protection law seeks to strike a balance between individuals' rights to privacy and the free flow of personal data. Data protection is a highly developed and regulated area of law.

Article 51 of the GDPR requires Member States to provide for an appropriate national competent authority for data protection. In the UK, this function is performed by the Information Commissioner's Office (ICO). One of the functions of the ICO is to provide guidance on data protection law compliance, which it has done extensively. At EU level, guidance is also issued by the European Data Protection Board (established under Article 68 GDPR).

1.2. What is personal data?

The GDPR and the DPA 2018 primarily govern 'personal data'. This is an important preliminary point in the context of football data analytics, as data analysts are likely to manipulate both personal and non-personal data in the course of their work. Personal data is defined in Article 4 of the GDPR as being 'any information relating to an identified or identifiable natural person', otherwise referred to as 'data subjects'. The concept of an 'identifiable' person is an important one. Article 4 states that a person is identifiable if they:

> can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Consequently, some more advanced performance data fields which do not directly identify a player may nevertheless constitute personal data within the ambit of the GDPR. Consider, for example, the data analytics insights from the article 'Running Stats Explained: Pace, intensity and the Premier League "Plodders"' in the Athletic (Worville, 2021):

- 'Aston Villa's Trezeguet is…topping over 80 high-intensity runs and sprints'. This is personal data. It contains information which directly identifies and concerns a natural person.
- 'a sprint is anything above 25.2 km/h, which is seven metres per second'. This is not personal data. It does not and cannot identify a natural person.
- 'the level of high-intensity running done by Leeds is clear and, as a group, unmatched by any other team'. This *may* constitute personal data. Leeds United Football Club is not a natural person; however, its team is, of course, composed of a narrow class of natural persons, i.e., those players in the Leeds squad who are selected to play. If, whether alone or in combination with other information available to a data processor, this team-level data could be reverse-engineered to reveal data concerning individual players, then the data may relate to an 'identifiable' natural person and thus constitute personal data. This illustrates the fact that information may be personal data when processed by one party (for example Leeds, being in possession of more granular data, may be able to use this statistic to identify information about individual players) whereas it may not be when processed by another party.
- 'The band before a sprint is a 'high-intensity run', which is where a player moves at between 19.2 km/h and 25.2 km/h…roughly how fast a grey squirrel can travel at top speed'. This is not personal data as a squirrel is not a natural person.

1.3. Categories of data and legitimacy of processing

Within the concept of personal data there is a distinction made in respect of 'special category data', which are:

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership…genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9, GDPR).

The processing of any personal data (whether or not special category) must only be performed where there is a lawful basis to do so (Article 6, GDPR). These lawful bases are broad: the consent of the data subject; necessity for the performance of a contract to which the data subject is a party; necessity for complying with a legal obligation; necessity to protect someone's vital interests; necessity for tasks carried out in the public interest or the exercise of official author-

ity; and where necessary for the legitimate interests of the controller. The basis on which personal data are processed in sport can be complicated. See for example Viret's assessment of the conflicts that arise in an antidoping context (Viret, 2019), Patel and Varley on the impact of data protection law on genetic testing (Patel and Varley, 2019), Hessert's analysis on data protection in sports regulatory investigations (Hessert, 2020a), and the impact of data protection in arbitration, *Barnsley Football Club Limited v Hull City Tigers, EFL (Ch Nicholas Stewart QC), 16 February 2021* (see paragraph 297).[3]

In the specific case of data analytics, the basis on which football's data analysts are able to process personal data will vary dependent on the particular facts. For example, a club may be able to rely on the 'performance of a contract' basis given the direct contractual relationship with its players.[4] However, the fact that data controllers are able to rely on their own legitimate interests in their use of player data will mean that there is a wide scope for data analytics organisations to legally process personal data, even where those organisations do not have a direct (or even an indirect) relationship with the data subjects in question (i.e., the players). 'Legitimate interests' are therefore a widely adopted basis for processing of personal data.

For proper data protection compliance, though, reliance on a data controller's legitimate interests is somewhat more complicated. As a starting point, data controllers must perform a 'careful assessment' (Recital 47, GDPR) as to whether relying on their legitimate interests is appropriate—it will not always be so. The recitals to the GDPR state that legitimate interests as a basis for processing can be relied upon: 'provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller' (Recital 47).

The legitimate interests of the data controller can be commercial. Recital 47 specifically gives direct marketing as an example of a data controller's legitimate interests, and ICO guidance states that:

> A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test. (ICO, 2021a).

ICO guidance on data controllers' legitimate interests (ICO, 2021a) suggests that data controllers should perform a three-part test:

a. The purpose test: determining whether a legitimate interest is being pursued.
b. The necessity test: determining whether the processing of the data in question is necessary for that purpose.
c. The balancing test: weighing the data subjects' interests against the interests of the data controller.

In the case of data analytics, the first two tests can likely be satisfied. Performing statistical analysis in football has benefits, be they sporting, scientific, or commercial; and it is inherent to the act of data analytics that data are processed. Therefore, whether the legitimate interests of data analysts can be relied upon will depend on a balancing assessment between the data analysts and the data subject players. The ICO gives guidance on the sort of questions that a prospective data controller may ask of itself in determining whether it is appropriate to rely on its legitimate interests, which include: 'Is any of the data particularly sensitive or private? Would people expect you to use their data in this way? Are some people likely to object or find it intrusive?' (ICO, 2021a). The ICO alludes here to the 'reasonable expectations' of the data subject, a factor mentioned in Recital 47 of the GDPR, which Kamara and de Hert (2018) suggest 'will be a significant element of the balancing test.' Given the public nature and scrutiny in respect of nearly all aspects of footballers' performance, these factors are likely to weigh in favour of data analysts, and players' reasonable expectations will surely be that the public may observe and analyse their playing performances, including in statistical format (after all, what is a league table or a top goalscorers chart if not a manifestation of statistics).

However, further questions asked by the ICO may fall more in favour of the players' overriding interests: What is the possible impact on the individual? How big an impact might it have on them? Are you processing children's data? Can you offer an opt-out?' (ICO, 2021a). Given factors such as the fact that data analytics may be used in player recruitment or player selection (thus having an influence on players' career opportunities), and that data sets may include information about children,[5] and that it would be difficult to offer a practicable opt-out to those players whose personal data are processed, the balancing act is clearly not a foregone conclusion in the analysts' favour.

So, where a legitimate interest can be relied upon will be subjective, requiring careful deliberation, and should be kept 'under review and [refreshed] if there is a significant change in the purpose, nature or context of the processing' (ICO, 2021a).

To complicate matters further, the bases on which special category data can be processed diverge from the bases on which other personal data can be processed. There is a restriction on the processing of special category data except where certain exceptions apply and, critically, the legitimate interests of the data controller are *not* a basis for processing special category data (Article 9, GDPR). This is a challenge for football data analytics given 'data concerning health' is classified as 'special category'. The GDPR defines data concerning health as 'personal data related to the physical or

mental health of a natural person…which reveal information about his or her health status'*;* the ICO construes this as including 'any related data which reveals anything about the state of someone's health' (ICO, 2021b). The nature of data analytics in football is such that there is an inherent risk that health information may be processed (or inferred) where players' physical performance is analysed.

The restriction on processing special category data does not apply, however, where 'processing relates to personal data which are manifestly made public by the data subject' (Article 9 (1) (e), GDPR). This is likely to square off many instances of data processing in the football analytics industry. Third party participants have access to data which, whether or not special category, are manifestly made public by players in their performances in matches; data relating to non-public player data, such as data relating to performances in training, will generally only be capable of being collected by parties with a direct relationship with the players, such as clubs, and thus may be processed on the basis of consent. Clearly, though, third party data analytics firms should be cautious in the receipt of personal data from other parties, and should seek appropriate contractual reassurance that any data transferred are received and capable of being processed in accordance with data protection law (further analysis on data transfers is set out below at section 1.7, below).

Where a direct player-analyst relationship exists, the reliance on consent as a legal basis for processing is no less complicated. Consent is defined in the GDPR as being 'freely given, specific, informed and unambiguous' (Article 4 (11)). This is difficult to establish where uneven power dynamics between data controllers (for example clubs or SGBs) and data subjects (players) are at hand. Recital 43 to the GDPR clarifies that consent cannot be a valid legal ground for processing where there is a clear imbalance between the data subject and the data controller. In some circumstances, this will make consent a troublesome basis for legitimising data processing. Gilchrist and Phelops (2017) suggest that 'data protection regulators, in certain jurisdictions, have formed the view that consent can never be validly given, for the purposes of data protection law, in the traditional employer / employee relationship (such as the one that normally exists between a football club and its squad).' Hessert (2020b) argues that the need for consent to be freely given is 'problematic in the sporting context, bearing in mind that sports events are often organised by monopolistic sports governing bodies'. This is a well observed point, and of course it has been a prevailing recent theme of sports law that the balance between what is consented to and what is unilaterally imposed have been keenly debated at the CAS, in the courts, and in the literature (see Duval, 2017).

Despite the tensions set out above, what can be taken from the assessment of the categories and legitimacy of processing in football data analytics is that there will generally be a legal basis for performing statistical analytics on players *available* to analysts, but participants in the data analytics ecosystem will need to carefully reflect on the basis and extent of the work they do, as compliance with applicable data protection law is unlikely to be straight-forward even where permissible.

1.4. Thresholds and territory

The GDPR, being an EU regulation, is directly effective in the 27 Member States, with its principles also incorporated into UK law by the DPA 2018. Its territorial scope, however, can effectively extend worldwide as the GDPR applies where processing of personal data:

- emanates from an EU established organisation, regardless of whether the processing takes place in the EU or elsewhere (Article 3(1), GDPR).
- relates to the personal data of data subjects in the EU where the data processor is outside of the EU, but either offers services (or goods) into the EU (Article 3(2)(a), GDPR), or the data processor monitors the behaviour of data subjects in the EU (Article 3(2)(b), GDPR).

These provisions are effectively replicated by section 207 of the DPA 2018,[6] supplanting 'the EU' with 'the UK'.

This wide territorial scope is important when you consider the global structures of the data analytics industry. Consider, for example, Arsenal's purchase of US-based data analytics company StatDNA (Hynter, 2014) (now known as Arsenal Data Analytics)[7]—whilst incorporated outside of the UK/EU, this US-based company may be construed as relating to the activities of a UK organisation (i.e., Arsenal), and/or relating to the provision of services into the UK (providing statistical analysis services to Arsenal) and/or may involve the monitoring of the (workplace performance) behaviour of UK and/or EU citizens (i.e., players), each of which would serve to bring its activities within the scope of the DPA 2018 (or as the case may be GDPR, or both).

Clearly, the focus of many analysts' data processing will be the EU and the UK, given Europe's place in the football ecosystem. This means that from a territorial perspective, the principles enshrined in the GDPR are likely to apply. There is an additional consequence to this in that, subject to limited exceptions, those parties outside the UK or EU who provide services into the EU and/or monitor the behaviour of EU data subjects must appoint a representative in the UK or EU (each as the case may be) (Article 27, GDPR).[8]

On the face of it, this is likely to bring nearly all football data analytics work into the scope of the GDPR. This may be of concern to some of those who participate in football data analytics, which is in many respects a nascent industry, with a strong culture of DIY 'fanalysts' and significant movement from fanalytics into professional data analyst positions.[9] Clearly, compliance with the full extent of the GDPR would be a near impossible burden for the typical fanalyst,

and significant impediment to the development of data analytics. Mercifully, for those involved, in data analytics on an amateur basis, there are threshold criteria and (partial) exemptions that will take most fanalysts out of scope.

As a starting point, the principles of the GDPR will apply where data processing has some degree of automation or where the data will form a part of a 'filing system', which is to say the data in question are structured in some coherent way (Article 2(1), GDPR; Article 4(6) GDPR). It suffices to say that most professional data analytics participants will satisfy these criteria—but casual, manual, *ad hoc* data analytics performed will not, and will thus not fall within the ambit of data protection law.

Even more systematic analytics work performed by non-professionals is likely to materially fall outside of the scope of the GDPR. The GDPR makes clear that it does not apply to the processing of personal data for 'purely personal or household activity' (Article 2(2)(c) and Recital 18, GDPR), and there are partial exemptions which apply to data processing for academic or journalistic purposes (Article 85, GDPR, incorporated in UK law under a 'special purposes' exemption under sections 174–176 DPA 2018). Where those exemptions do not apply, there is also a limited exemption (Article 30(5), GDPR) for organisations of 250 persons or fewer whose data processing is occasional, does not include special category data, and is unlikely to result in a risk to the rights and freedoms of data subjects. Once data analytics becomes systematised and professionalised, it is unlikely that these exemptions will apply.

1.5. Principles of data protection

Where the GDPR (or DPA 2018) applies to the data controlled by a participant in the data analytics ecosystem, that data controller will be responsible for ensuring the core data protection principles are applied. The principles, set out in Article 5 of the GDPR, go to the heart of the EU and UK data protection regime, and state that data must only be processed:

a. lawfully, fairly and transparently
b. only for specified, explicit and legitimate purposes
c. in accordance with the principles of data minimisation
d. accurately and kept up to date
e. for no longer than is necessary; and
f. with integrity and confidentiality.

Compliance with these requirements is a fundamental obligation for the systematised manipulation and exploitation of player performance data, and should therefore form an integral part of any data analyst's processing. It is important to note that these principles extend beyond merely what one does with personal data—they apply to 'the whole continuum of data processing, from the stage when data is first acquired….to the time when it is permanently and irretrievably destroyed' (Lloyd, 2020, p. 71). Consider, for example, the obligation to process personal data with integrity and confidentiality. This necessitates putting in place appropriate information security provisions. This applies against the background of the football industry as a whole having experienced several data leaks: Consider 'Footy Leaks' and its impact on the Manchester City Financial Fair Play dispute (Flanagan, 2020), the Liverpool and Manchester City hacking dispute referred to in Part One, section 2.2.4.1 of this article, leaks of supporter personal data by West Ham (Collins, 2021), or the cyber attack on Manchester United (Guardian, 2020). The National Cyber Security Centre has produced a report on the cyber risk threat to sports organisations (National Cyber Security Centre, 2020).

Beyond the specific case of sports data, the GDPR's data protection principles are sometimes depicted as being antithetical to data analytics. Consider, for example, the intersection of the data minimisation principle with the necessity for large data sets on which data analytics is dependent; however, as Stalla-Bourdillon and Knight (2018) argue, 'the GDPR is also intended to be a trust creator and a data sharing enabler for the purposes of innovation fostering…through promoting context-driven risk analyses, which in turn requires organisations to be more transparent about their personal data processing practices'.

1.6. Controllers and processors

In recognition of the differing roles played by actors in data ecosystems, UK and EU law compartmentalises parties into categories of 'controllers' and 'processors'.[10] Risks, roles and responsibilities under data protection law vary dependent on whether a party using personal data does so as a controller or a processor.

A controller is a 'body which, alone or jointly with others, determines the purposes and means of the processing of personal data' (Article 4(7), GDPR). Data can be controlled by one party, by multiple parties separately, or by multiple parties jointly (where for example there is a common data set, Article 26, GDPR; for further exploration see Tran and Adde, 2019). By contrast, a processor is a 'body which processes personal data on behalf of the controller' (Article 4(8), GDPR). In practice, these distinctions are not as clinical as their definitions seem, and a typical data sharing arrangement will (and often *should)*[11] involve an assessment as to the roles the relevant parties play in the relevant data ecosystem. This is important for two particular reasons: firstly, to ensure that each party performs in accordance with the data protection law as it applies respectively to controllers and processors, as the obligations diverge; and secondly, to ensure that data are shared lawfully, as data must only be processed by a data processor on a controller's behalf pursuant to contract (or 'other legal act' under EU or Member State law), in which the contract must contain certain prescribed

obligations (Article 28(3), GDPR). There is no absolute legal obligation for data controllers to share data between one another pursuant to a contract,[12] although to cover this lacuna, the ICO has published a data sharing code of practice which makes clear that it is good practice to have in place a data sharing agreement in place (ICO, 2020a).

The risks presented by this taxonomical approach to data protection law are of course not idiosyncratic to sports data analytics, but the underlying distinctions are central themes to data protection compliance where there are multiple participants in a data ecosystem, such as where a dedicated data analytics firm produces data insights based on data collected by a club (on general issues outside of data analytics see for example Oastler, 2018; de la Cruz, 2020).

1.7. International data transfers

It is not only the transfer of personal data between controllers and processers that is subject to specific legal obligations under data protection law. There are also detailed requirements in respect of international transfers (of personal data rather than players—although international player transfers will usually entail some international personal data transfers, for example via the FIFA TMS system). This is important for many facets of sport (see for example Kornbeck, 2017; Kornbeck, 2020), and particularly for present purposes in the context of football's data analytics movement, which, like the industry it serves, is globally distributed.

The GDPR states that personal data may only be transferred to a third country—that is any country other than a Member State or the three additional European Economic Area states which have adopted the GDPR—where certain conditions are satisfied. This position is further complicated by Brexit, which, but for transitional measures,[13] rendered the UK a third country for GDPR purposes; and recent case law, which imposes additional impediments on personal data transfers to third countries. Conversely, for exports from the UK, any country outside the UK will be a third country.[14]

A transfer of personal data to a third country is only permissible where certain criteria are met. The first such is where an adequacy decision has been made in respect of that third country by the European Commission or the UK Secretary of State for Digital, Culture, Media and Sport (as applicable), although a limited number of such decisions have been made (European Commission, 2021). In the absence of an adequacy decision, transfers must generally[15] only be made where prescribed 'appropriate safeguards' are put in place (Article 46, GDPR) and provided that 'enforceable data subject rights and effective legal remedies for data subjects are available' in the recipient state (Article 46(1), GDPR). A number of appropriate safeguards are set out in the GDPR, with the most commonly used in a commercial context being 'standard contractual clauses' (a form of contractual clauses in the exact form specified by the European Commission, UK Secretary of State, or ICO as applicable), less commonly,[16] 'binding corporate rules' (a set of binding policies which govern data transfers within a corporate group (Article 4(20), GDPR)).

This compliance burden is complicated further by the decision in *Data Protection Commissioner v Facebook Ireland Ltd (C-311/18) [2020] 7 WLUK 245 (ECJ (Grand Chamber))*, commonly referred to as '*Schrems II*'. The headline findings of the ECJ in *Schrems II* were the invalidity of the 'Privacy Shield'—an adequacy framework for EU-US data flows approved by the European Commission—and the validity in abstract terms of the Commission's standard contractual clauses (SCCs). However, exporters of personal data to third countries 'must ensure that the rights of the persons whose data are transferred benefit…from a level of protection essentially equivalent to that which follows from the GDPR' (paragraph 115, *Schrems II*) and cannot rely on the SCCs alone in ensuring this. Consequently, for data exporters 'not only must the terms of the SCCs themselves be taken into account but also the general legal environment in the destination State' (Woods, 2020). Despite the existence of the Privacy Shield, the position as regards data transfers from the EU to the US was found to insufficiently protect data subjects' rights. Woods (2020) states that this also 'has consequences for the operations of SCCs in practice at least as regards transfers to the US because it implies a negative assessment of the US data protection standards'. So, the export of personal data to the US is challenging per se; however, the consequences of the decision in *Schrems II* go beyond the flow of data to the US. The assessment of local law in the data importer's jurisdiction will apply where the SCCs are relied upon. This results in 'the imposition of a form of due diligence obligation on those controllers no matter the destination to which the data are transferred' (Woods, 2020).

In the global world of football data analytics, this means that data collected by a club or league in the UK or EEA cannot be transferred to (say) a data analytics company in a third country, such as the US, in reliance on the SCCs without also performing an assessment of that country's prevailing privacy law framework—which in the specific case of the US has already been viewed unfavourably by the ECJ. Moreover, data analytics firms who post information and insights online will in likelihood be construed as transferring data to third countries (see *Lindqvist v Aklagarkammaren i Jonkoping (Case C-101/01) EU:C:2003:596*) unless they can do so in reliance on the partial exemption for journalistic or academic purposes described in section 1.4, above.

1.8. Data subject rights

The fundamental purpose of the restrictions on data transfers to third countries is to protect data subjects' privacy rights by ensuring that data are not transferred to territories with lower data protection standards (see *Schrems II*).

The rights of data subjects are further protected by specific data subject rights, which may affect those who wish to monitor and manipulate data relating to football players' performances. Data subjects' rights are set out in Chapter 3 of the GDPR and the DPA 2018 respectively. These rights can be split into two loose categories: 1. rights to information in respect of personal data usage; 2. rights of personal agency in respect of third parties' use of data concerning that individual.

1.8.1. Information rights

Uses of personal data should be transparent. The GDPR ensures this in two ways: by compelling data controllers to disclose to data subjects details on the information collected, whether or not collected directly from the data subject (Article 13, GDPR) or from another source (Article 14, GDPR) (this disclosure is commonly referred to as a 'Data Privacy Notice', or DPN); and by compelling data controllers to provide to the data subject information on and copies of the data held by the data controller in respect of that data subject, commonly referred to as a 'Subject Access Request', (SAR or DSAR).

Practically speaking, the provision of a DPN may be challenging in the context of the football industry, particularly in respect of third party data analytics firms, who may not have a practicable way of, say, informing Andros Townsend that they are collecting information on the number of shots he takes from prime locations per game. There are exceptions that apply to the requirement to provide a DPN where data are collected from third party sources, and of most practical use in the case of football data analytics will be the exception in Article 14(5)(b) GDPR, where 'the provision of such information proves impossible or would involve a disproportionate effort'. However, in order to rely on this exception, the data controller must 'take appropriate measures to protect the data subject's rights and freedoms and legitimate interests',[17] which includes 'making the information publicly available'. Clearly, this may be unpalatable to data analysts where the fidelity of the data in question has commercial or sporting value.

Generally speaking, the obligation to provide SARs will be less problematic for data analysts—although a bureaucratic burden—requiring the provision of a copy of the data held by the controller concerning the data subject, and information on the processing that is performed, to that data subject (Article 15, GDPR).

1.8.2. Data subjects' personal agency

Irrespective of the rights that data controllers may have to process players' personal data without express consent, any such use will in principle be subject to the principles of players' personal agency in respect of those data enshrined in the GDPR.

These rights are: the right to rectification of inaccurate or incomplete personal data (Article 16, GDPR); the right to data portability (Article 20, GDPR); the right to erasure, sometimes referred to as the right to be forgotten (Article 17, GDPR); the right to restrict data processing (Article 18, GDPR); and the right to object to the processing of the data subject's personal data (Article 21, GDPR).

These are qualified rights, in that they do not apply in all circumstances, and do not provide an unfettered right for data subjects to prevent all data processing to which they are subject from occurring. However, in light of Project Red Card,[18] and in view of protestations by Gareth Bale and Zlatan Ibrahimovic in which they publicly objected to the use of their image (rather than data per se) under the hashtag #TimeToInvestigate (The Athletic, 2021), the rights of players to restrict or object to the processing of their personal data is contentious.

Importantly, the right to object to the processing of personal data arises where the lawful basis of the processing of that data relied on by the controller is the legitimate interests of that controller (or another third party) (Article 21(1), Recital 69, GDPR). In such circumstances, a data controller would be obliged to stop the processing of the player performance data in question unless it could demonstrate 'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.' (Article 21(1), GDPR). Generally, where a right to object to the continued processing of personal data arises, there will be a corresponding right of erasure in respect of the other personal data which the data controller in question may have in its charge. Aside from the relationship between players and third party data processors, this provides an interesting answer to Greenbaum's question 'Can an athlete legally limit his or her opponent's access to helpful data?' (Greenbaum, 2019): potentially yes, unless the opponent can establish that their competitive rights override the interests of the player.

The portability right applies to limited data sets (data processed pursuant to the data subject's consent or where necessary to perform a contract) and in limited circumstances (only to data processed by automated means), but this may nevertheless prove challenging to clubs where players transfer to new teams, given that strategically sensitive data analytics may fall within the narrow ambit to which portability applies (Article 20, GDPR).

Players also have the right not to be subject to decisions—for example, player recruitment decisions—based solely on automated processing or profiling.[19] Ordinarily, one would not anticipate that clubs would make player sale or recruitment decisions based *solely* on data analytics, although as the balance shifts towards a more data-orientated approach, this data subject right should be borne in mind.

1.9. Accountability and governance

In addition to establishing the specific rights and obligations of the participants in a data ecosystem, the GDPR also establishes high level accountability and governance obligations. In addition to being accountable for ensuring compliance with the six data protection principles set out in section 1.5 above, the GDPR requires data controllers to ensure that data privacy is embedded by 'design and by default' (Article 25, GDPR). The European Data Protection Board makes clear that this obligation arises 'early on…before processing, and also continually at the time of processing' (European Data Protection Board, 2020).

The obligation for data controllers to self-reflect in this way is hard-wired into the GDPR. Article 35 of the GDPR requires controllers to perform data protection impact assessments (DPIAs) where processing activities precipitate a high risk to the rights and freedoms of data subjects. In particular, this should be performed where the processing in question involves 'processing on a large scale of special categories of data' (Article 35(3)(b), GDPR), such as player health information, or involves 'a systematic monitoring of a publicly accessible area on a large scale' (Article 35(3)(c), GDPR). Given the nature of data analytics, it is likely that a significant amount of data analytics work will necessitate a DPIA being performed. In *R (Bridges) v Chief Constable of South Wales Police (Respondent) and others [2020] Civ 1058*, a case in which automated facial recognition technology was found to have been deployed by police in breach of human rights and data protection law, defects in the police's DPIA were pivotal to the relevant breaches of law (paragraph 153, R (Bridges)).

In order to ensure proper data privacy governance, certain organisations are under an obligation to appoint a data protection officer (DPO), who must be appropriately qualified with an 'expert knowledge of data protection law and practices' (Article 37(5), GDPR), and who must report to the 'highest management level' (Article 38(3), GDPR) of the organisation. The DPO is charged with advising on, and monitoring compliance with, data protection law. The obligation to appoint a DPO is not absolute, but organisations must do so where their 'core activities…by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale' (Article 37(1)(b), GDPR). Given the nature of data analytics, this is likely to encompass many organisations at which data analytics occurs.

Failures to comply with data protection law have the potential to create both civil and administrative liabilities. From a civil liability perspective, Article 82(1) of the GDPR states that 'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'. In English law, the position regarding what constitutes 'damage' on the one hand (see Roughton, 2019; Janeček, 2020), and a rise in class action data litigation on the other (Hopkins, 2019; Chapaneri, 2020; Castro-Edwards, 2021) has rendered the position uncertain for data controllers and processors.[20] Where breach and damage are established, the position in respect of quantum of damages is also presently somewhat uncertain.[21]

Irrespective of the uncertainty around civil liability, the position in respect of administrative fines is clear: sanctions for breaches can be severe—up to the greater of €20m or 4% of worldwide turnover in the prior year (Article 83, GDPR)—and in the UK, the ICO has, at the time of writing, already issued several multi-million pound notices of intent to fine for breaches of the GDPR (Hasan, 2020).

1.10. FIFA's Data Protection Regulations

In 2019, FIFA adopted its own Data Protection Regulations (FIFA DPRs, FIFA 2019). The FIFA DPRs have considerable conceptual overlap with the GDPR, with many of the GDPR's main themes—on data protection principles, on data subject rights, on data privacy information—ostensibly adopted from the GDPR, albeit with some minor deviations and in a considerably more slimline format.

In contrast to the GDPR, the scope of the FIFA DPRs is quite narrow, relating only to personal data processed by, on behalf of, or with FIFA; where exchanged with FIFA or a FIFA Member Association; or where relying on infrastructure provided by FIFA. It expressly does not include personal data processed by Member Associations or their members 'using their own infrastructure; for their own purposes; and in their own right' (Regulation 3, FIFA DPRs).

The FIFA DPRs are interesting in that they incorporate data protection principles directly into the lex sportiva,[22] reflecting Weatherill's (2021) observation that: 'the economic centrality of Europe to many, if not all, sports means that in practice the need to adjust practices to comply with EU law sometimes entails that adjustment operates more widely. EU's norms become global norms.' However, for the purposes of data analytics, the impact of the FIFA DPRs is likely to be minimal, given the necessary nexus with FIFA in order for the FIFA DPRs to apply.

For more detailed analysis of the FIFA DPRs and its distinguishing features from the GDPR, see Bellamy (2020).

1.11. Data protection law and sports data – conclusions

In basic terms, there is scope for data analysts to use and manipulate player performance data. In many circumstances this will not entail seeking the permission of the player in question. However, data analysts will only be able to perform their activities where they do so in compliance with data protection law. This will entail the navigation of a dense network of law and regulatory guidance. For UK based analysts who monitor the data activities of EU data subjects, or vice versa, this may entail compliance with both UK and EU data protection law as it bifurcates post-Brexit. This is a complex task which requires careful consideration, and in likelihood some compliance costs, which may act as an impediment to new market entrants in the data analytics space.

Inversely to the position in respect of intellectual property rights in data analytics, the legal rights associated with the exploitation of player data lie primarily with the players rather than the data analysts. Notwithstanding the prima facie rights that analysts may have as data controllers, rights of objection, restriction, and erasure present potential problems for data controllers who rely on their own legitimate interests to process that data, whereas controllers who rely on consent are prone to that consent being withdrawn.

In that regard, Project Red Card presents an issue on two levels: Firstly, it highlights the autonomy players have if they choose to exercise their rights over their personal data on a systematised basis; secondly, it presents a potentially significant liability for any users of player personal data who have done so without adhering to the detailed obligations set forth in the GDPR.

Hessert (2020b) highlights the fact that athletes, as data subjects, have a right to compensation under Article 82(1) of the GDPR, in circumstances whereby their personal data are exploited without an appropriate legal basis. This is by no means a *fait accomplis* vis-à-vis data analytics, as participants in the football data analytics community do have scope to utilise player performance data, even in circumstances where they are pursuing their own commercial interests, without the consent of players. However, this can only be done in compliance with the prevailing data protection law and regulation, which is a complex activity requiring detailed and ongoing consideration and self-reflection. In a nascent analytics market, this will necessitate a degree of organisational maturation in order to ensure that players' data rights are not infringed.

2. Other legal issues

Whilst intellectual property and data protection law are the two most prominent themes when considering the legal issues confronting football data analytics, they are not the limit of the issue. Many of the points mentioned in this section may warrant further exploration as the football data analytics industry develops, or as legal issues in respect of other uses of sports data have transversal application to data analytics, in the same way that sports betting data has framed intellectual property use cases.

2.1. Competition Law

Competition law has been a central theme of the regulation of the football industry. Gardiner et al. (2012: 64) describe it as 'the most significant aspect of EU law germane to the sporting context'. Given the structure of sport, and the potential for monopoly rights to be exerted in the collection of data (see section 2.2.4.2 of Part One of this article describing the 'house right'), or the potential for competitors to be excluded from data markets by agreements or conduct, there is scope for breaches of each of Articles 101 and 102 of the Treaty on the Functioning of the European Union (or their closely aligned domestic counterparts in UK law, Chapters 1 and 2 of the Competition Act 1998), which govern agreements restrictive of competition and abuses of dominant positions respectively.

In the specific case of sports data, competition law issues may arise in several key risk areas. Firstly, information sharing. Where confidential sports data are exchanged between competitors and those data give an indication as to future strategy. For example, a systematised sharing of player training data between leading clubs would warrant additional consideration from a competition law perspective. Secondly, harmonisation. Where a majority of competitors take data from a single source, or rely on the same data processing mechanism (say, a specific algorithmic process), this may impact the competitive functioning of the market and will warrant vigilance for competition law compliance. And thirdly, discrimination. Any agreement to exclude certain competitors from access to data sets or data-derived sporting advantage should be treated with caution. This issue may arise, for example, in exclusivity arrangements between data analytics organisations and their club clients–particularly if the analytics firm has a dominant market position, or access to data that become critical to enable clubs to compete.

Indeed, competition law has already become a point of contention in the sports data market, specifically in respect of the exercise of the 'house right' described in section 2.2.4.2 of Part One of this article: The Competition Appeal Tribunal case of *Sportradar AG and Sportradar UK Limited v Football DataCo Limited, BetGenius Limited and Genius Sports Group Limited (Case no 1342/5/7/20)* concerns a challenge by the claimant sports data group, Sportradar, in respect of contracts concerning 'official' data collection and distribution rights between Football DataCo and Genius, a competitor of Sportradar's, on the basis of both Articles 101 and 102 of the Treaty on the Functioning of the European Union.

2.2. Regulation of Artificial Intelligence

On the horizon for football's data analytics community should be the EU's draft AI regulation (the Draft EU AI Regulation), which is proposed to provide a comprehensive risk-based framework for AI, which will act as a 'uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values' (Recital 1, Draft EU AI Regulation) (European Union, 2021). The Draft EU AI Regulation draws on a broad definition of AI, including 'machine learning approaches…logic and knowledge-based approaches… [and] statistical approaches' (Annex 1, Draft EU AI Regulation), and of particular relevance to football data analytics is the designation of certain systems as being 'high risk' and thus attracting greater levels of regulatory oversight. This includes 'AI systems intended to be used for recruitment or selection' and 'AI intended to be used for making decisions on promotion and termination of work-related contractual relationships' (Article 6(2) and Annex III, Draft EU AI Regulation), which are core data analytics use cases. The specific text of the Draft EU AI Regulation is likely to change as it moves through the legislative process; however, it is sure to stress appropriate governance, transparency, and human oversight and accountability in the use of AI which affects employment relationships.

Of course, the use of AI in data analytics, insofar as it involves the processing of personal data, is already subject to data protection law, and indeed the ICO has published Guidance on AI (ICO, 2020b). Much like any complex personal data usage, regulatory compliance when using AI for football data analytics should be considered at an early stage. As Fierens and de Bruyne (2020) conclude: 'There are several legal and ethical challenges regarding the use of AI-systems in sport'; but good governance and compliance-orientated practice in football data analytics should ensure that AI can continue to be used for the betterment of the sport.

2.3. Other legal issues

A number of other legal issues may arise from data analytics in football. The intersection of human rights and data protection law was touched upon in section 1.9 above, and Article 8 of the European Convention on Human Rights, which protects private and family life, home, and correspondence may be engaged where an employer undertakes systematised surveillance of an employee's workplace behaviour (see *Bărbulescu v Romania, ECHR [2017]*); similarly, such monitoring in the context of the power dynamic of an employer-employee relationship such as a typical club-player relationship may give rise to employment law concerns.

Data analysts may concern themselves with issues of product liability, and in an industry which is built upon an ability to derive value through objective insight, analytics-based advice may in particular give rise to issues in tort or contract of negligent misstatement or negligent misrepresentation in circumstances where negligent recommendations on player recruitment are made and those recommendations are relied upon by clubs.

Finally,[23] as with all legal issues in sport, the compulsory system of arbitral dispute resolution under which football operates (as to which, see Duval, 2017) may have legal implications for football data analytics–particularly given those fora are used to determine matters which may be within the purview of data analytics, such as a player's market value (consider historically, for example, *FC Shakhtar Donetsk v. Matuzalem & Real Zaragoza SAD (CAS 2008/A/1519); Udinese Calcio S.p.A. v. de Sanctis & Sevilla FC SAD (CAS 2010/A/2147); Mutu v. Chelsea Football Club Limited (CAS 2008/A/1644*). Data protection issues are 'gradually arising in the CAS proceedings' (Novak and Kühne, 2020) in the context of anti-doping proceedings, and indeed have arisen in arbitral matters relating to player transfers (*Barnsley Football Club Limited v Hull City Tigers)*. Data protection issues at the CAS may shape data analytics by influencing the approach to data taken by data issues in light of the jurisprudence of the CAS[24] and by presenting the data analytics industry with opportunities to provide objective measures to sports disputes, such as in the form of expert witness testimony (as to which, more generally, see Rigozzi and Quinn, 2014; Coleman and Taylor, 2020).

3. Conclusions

Digital transformation, analytics, and its symbiosis with big data is a recurrent theme across a number of industries. Football has not escaped this. Data analytics has become an important facet of elite football, creating on-field competitive advantage and commercial opportunities to those who are best able to leverage its uses. Inevitably, in the zero-sum world of professional football, where the success of one club is mutually exclusive to the success of another, disputes will arise over data access and exploitation. Moreover, given that data analytics is predicated on the processing of personal data of players, who may or may not consent to, or even be aware of, the processing of their personal data, this gives rise to clear points of friction in the world of football data.

The legal framework in which player performance data sits creates the opportunity for many innovations to be protected by intellectual property law, and the use of the underlying data will not in all circumstances be prevented by, or rely on express player consent for compliance with, data protection law.

Conversely, there is no property in the constituent data on which data analytics relies, nor any inherent right to use player performance data merely because it is in the public domain. The GDPR applies in full whether or not data are publicly available, and the ICO has been clear on this point:

> The fact that personal data is publicly available does not mean that individuals no longer have the right to be informed about any further uses of their information. If you obtain personal data from publicly accessible sources…you still need to provide individuals with privacy information, unless you are relying on an exception or an exemption. (ICO, 2021d)

The position will, therefore, depend on the specific actions of the specific data user on a case-by-case basis and from time to time. Project Red Card, as an initiative to defend players' rights in the data that has been industrialised by football and its adjacent industries, will therefore succeed or fail based on specific instances of non-compliance where they can be identified.

As the multiplicity of cases discussed in Part One and Part Two of this article show, the legal battle for data primacy is well established, particularly in the context of exploitation for betting purposes. However, new technologies bring with them new paradigms. To date, the issues in dispute have related to data observable to fans watching in the stands or on television; players may have a legitimate expectation that these data—shots, passes, goals—will be collected and considered. The future, though, brings with it the prospect of the hyper-quantified athlete, in respect of whom more invasive data are collected, and whose information is processed in more sophisticated ways.

This brings with it policy concerns as well as legal and regulatory compliance issues. To that end, FIFPro, the global players' union, has taken an active role in establishing a data use and exploitation agenda on behalf of players. In 'A Future Oriented Player Data Policy For the Digital Football Industry', FIFPro sets out five priorities to 'govern the collection, protection and use of player data' (FIFPro, 2020). These are: 1. The establishment of a common interest between stakeholders, including players, of the advancement of data uses and technologies; 2. The establishment of collective data collection, protection, and use standards; 3. Ensuring that player data collection is purpose driven and in line with established data management standards; 4. Ensuring that players are adequately and directly compensated in respect of the commercial exploitation of data pertaining to them; and 5. Awareness and education initiatives.

Broadly, these policy initiatives follow the legal and governance trends in data; however, the fourth policy, proposing a mandate for players to take a monetary share in the usage of information pertaining to them, would take a shift in practices, as this is not generally how the data economy currently works. Establishing equilibrium in this respect will also take a careful balancing of the promotion of innovation to foster the mutual interest of data analysts and their subjects in advancing data analytics, since 'Players have an inherent interest and commitment to drive their performance through state-of-the-art technology' (FIFPro, 2020), with FIFPro's notion that 'Player Data is not public information, available free of charge' (FIFPro, 2020).

From a sports regulatory perspective, the possibility for asymmetries of power to be occasioned by advances in data analytics should also draw scrutiny; and, of course, those asymmetries of power transcend the club/player dynamic. As Hutchins (2016) states, 'For those sitting on the wrong side of this divide, including many women's sports, the seemingly intractable inequalities of television coverage, news reporting, and sponsorship investment that took root in the age of mass media are continuing'. Access to the vanguard of data analytics typically accrues to the wealthiest, which risks entrenching a wealth divide between rich and poor that already exists and is widening. Data, however, could equally be a solution to this issue, allowing economically disenfranchised clubs to overcome traditionally wealth-derived advantages. There are localised instances of progressive practices in this respect. For example, analytics firm Statsbomb has provided free access to data relating to certain women's competitions (Randall, 2018). However, reliance on piecemeal initiatives of this nature will likely be insufficient on their own, and a more institutional position on access to data analytics should be considered.

To that end, the early manoeuvres of FIFA and FIFPro towards a framework for data use and exploitation in football should be encouraged. In the specific case of FIFA, the implementation of the FIFA DPRs, along with segments on data analytics in its FIFA Professional Football Journal (FIFA, 2020b) indicate an institutional cognisance of the issues presented by personal data usage and its specific use case in data analytics. As the apex regulator of the game, FIFA is the best placed (and perhaps only) organisation to promulgate and cascade data use standards in football globally. Although the existence of a wide range of third party football data users outside of FIFA's direct regulatory ambit is likely to mean that its influence in some cases will be no more than hegemonic, that influence *is* capable of being given legal effect through chains of contracts. For example, where clubs purchase data analytics services from third party providers, the standards of football's governing bodies can be imposed on those clubs in respect of those services through the regulatory pyramid to which clubs are subject.

The benefits of data analytics in football are clear and manifold, allowing for technological advancement, efficiencies in recruitment, improved player load management, increased supporter engagement, and so on. This is acknowledged by FIFPro (2020). But the systematised use of player data does bring with it legal and ethical questions, particularly as information systems increase in sophistication and the scope of data collection increases with it.

The legal position in respect of Raw Data (as defined and set out in Part One of this article) is instructive: it is incapable of ownership, either by players or by those who observe them. What is left is a dispute around the governance of how those data are used. As Gilchrist and Phelops (2017) state:

> More now than ever, sports businesses, rights owners, governing bodies, federations will need watertight data protection policies and procedures, robust contractual terms with third parties who may process this data for them, clear notice and consent mechanisms with individuals (including their players), best practice technological means to keep this data secure and will need to consider what internal and external compliance function they will need to keep them the right side of the line.

Irrespective of strict legal rights, the tension between players and those who wish to exploit their data must be resolved by social dialogue. Project Red Card is headline news, but its outcome will in likelihood be determined by the idiosyncratic application of data compliance, and will likely neither liberalise nor foreclose the processing of player performance data per se.

The future of player data, and with it the future of data analytics in football, should therefore continue to be subject to compliance with applicable exogenous regulatory systems, and further buttressed by suitable endogenous regulatory systems, balancing advancement with players' interests in the information which concerns them. To that end, the public ventilation of the issues concerning the use of player data engendered by Project Red Card is a positive development—provided that the expected goals of the project are to move towards egalitarian legal and ethical governance structures to future-proof the game in light of advances in player monitoring and data science.

Notes

[1] FIFA 2019 *Data Protection Regulations*. [online] Available at <https://resources.fifa.com/image/upload/fifa-data-protection-regulations-2019.pdf?cloudid=dr9labmtd63ctx6o3erk> [Accessed 10 July 2020].

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] Barnsley Football Club Limited v Hull City Tigers, EFL (Ch Nicholas Stewart QC), 16 February 2021. Available at: https://www.efl.com/siteassets/image/202021/judgements/redacted-final-award-barnsley-v-hull-tue-16-feb-2021.pdf (last accessed 18 May 2021).

[4] Players' employment contracts will typically include provisions relating to the processing of personal data. See for example the pro forma form of player contract at Form 15, clause 21 of the Premier League Handbook Season 2020/2021: "For the purposes of the Data Protection Act 2018 and the General Data Protection.
Regulation ("GDPR") the Player acknowledges that the Club, the League, the PFA and The FA are collecting, sharing and otherwise processing Personal Data which may include Special Categories of Personal Data (both as defined in the GDPR) about the Player including such data in this contract. Premier League, 2020. Premier League Handbook Season 2020/2021. p.334. Available at <https://resources.premierleague.com/premierleague/document/2021/03/24/20a9c091-be5a-4bf5-a9f4-87e2a86ad84f/2020-21-PL-Handbook-240321.pdf> last accessed 7 April 2021.

[5] Noting in particular that the legitimate interest basis specifically refers to instances "where the data subject is a child" (Article 6 (1) ((f), GDPR), and the ICO, relying on the UN Convention on the Rights of the Child, defines a child as being anyone under the age of 18, which will mean a number of active professional players are 'children' for the purposes of data protection law – see ICO.org.uk. 2021. *Children and the UK GDPR*. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/> [Accessed 4 May 2021].

[6] As amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/485 to accommodate Brexit.

[7] Formally AOH-USA, LLC, as subsidiary of Arsenal Holdings Ltd.

[8] For more detailed exploration of the territorial issues associated with the GDPR and the DPA 2018, including in respect of the appoint of UK/EU representatives, see Bartoszewicz-Rawlinson, A. and Given, P., 2021. EDPB's Guidelines on Territorial Scope – Clarifications and Uncertainties. *Privacy & Data Protection*, 20(4), 5–7.

[9] Consider, for example, the incredible story of Ashwin Raman, the seventeen-year-old data analyst from India, whose blogs and tweets helped him to secure a job with Dundee United; or see more generally Biermann, C., 2019. Football Hackers. London: Blink Publishing.

[10] For historic detail on the distinction between controllers and processors, see the EU Article 29 Working Party's Opinion 1/2010 on the concepts of "controller" and "processor" (16 February 2010) available at <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf> accessed 26 April 2021.

[11] Dependent on the specific circumstances, data controllers may be obliged to perform a data protection impact assessment, appropriately mapping the flow of data and understand the roles each party in the ecosystem plays (Article 35, GDPR).

[12] Controllers must however only share data where it is otherwise permitted in accordance with data protection law – for example there must be a lawful basis for processing.

[13] Pursuant to the UK-EU trade and co-operation agreement implemented into UK law under the European Union (Future Relationship) Act 2020.

[14] Per Article 4(26) of the UK retained provisions of the GDPR, as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419.

[15] Transfers may also be made where derogations apply (Article 49, GDPR). These derogations are:

"(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case."

[16] Per Waiting, M (2020), "Binding Corporate Rules remain quite rare". Waiting, M. 2020. Top ten data protection considerations when outsourcing. Privacy & Data Protection, P. & D.P. 2020, 20(7), 3–5.

[17] The ICO suggests that if a DPN cannot be provided, a DPIA should be performed (ICO, 2021c).

[18] Per Part One of this article, "under which it is reported that legal action has been initiated by 'More than 400 current and former players…[against] betting and data-processing companies who utilise their personal statistics without consent or compensation' (Ornstein, 2020)."

[19] This right applies unless the automated decision in question, "(a)is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent." (Article 22(2), GDPR). Moreover, profiling must not be based on special categories of personal data unless one of the following conditions applies: (i)The data subject has given their explicit consent to that processing (Article 9(2)(a), GDPR); (ii) the processing is necessary for reasons of substantial public interest (Article 9(2)(g), GDPR), (Article 22(4), GDPR).

[20] See also the case of *Various Claimants v WM Morrison Supermarkets Plc* ([2020] UKSC 12), the first class-action data privacy case to be heard pursuant to a data breach.

[21] Knight (2021) reasons that "As to quantum of compensation, the GDPR gives us no real clue as to whether the existing case law is too generous, too restrictive, or about right… One might also note the placement of Article 82 alongside the administrative fines in Article 83, and the extremely high statutory maximums in that context, and infer that compensation (inevitably on a smaller and more individual scale than a regulatory sanction) ought at least to be in the same book, even if they are not on the exact same page."

These issues coalesced in the case of Lloyd (Respondent) v Google LLC (Appellant) [2021] UKSC 50, which, Knight (2021) posited "could have implications for Article 82 of the GDPR and the DPA 2018, potentially extending the scope of representative class actions exposing controllers and processors to large claims for compensation based on a breach of the data protection legislation alone and change the way in which representative class actions are brought in the UK by instigating an opt-out form of litigation rather than opt-in". However, in its judgment of 10 November 2021, the UK Supreme Court did not allow the representative action sought to proceed.

[22] Taking 'lex sportiva' here to include the system of administrative rules and regulations put in place by sports governing bodies. For more detailed consideration on the scope of the term, see Foster (2016), Foster (2019).

[23] Finally for present purposes–although the ability of the law and sport to convene and bring surprising new angles to matters should not be underestimated.

[24] Notwithstanding the lack of a formal system of stare decisis, as Blackshaw notes– "in the interests of comity and legal certainty, they are usually prepared to [follow prior decisions of the CAS]" (Blackshaw, 2003). For an empirical analysis, see the chapter CAS Decisions as Precedent in Lindholm (2019), pages 85–117.

Competing Interests

The author has no competing interests to declare.

References

Books

Biermann, C 2019 *Football Hackers*. London: Blink Publishing.

Gardiner, S *et al.* 2012 *Sports Law*. 4th ed. London: Routledge, p. 64. DOI: https://doi.org/10.4324/9780203180884

Kamara, I and **De Hert, P** 2018 *Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*. In E Selinger, J Polonetsky, and O Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (Cambridge Law Handbooks, pp. 321–352). Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781316831960.019

Kuschewsky, M 2016 *Data Protection & Privacy*. Sweet & Maxwell.

Lindholm J 2019 *CAS Decisions as Precedent*. In: The Court of Arbitration for Sport and Its Jurisprudence. ASSER International Sports Law Series. TMC Asser Press, The Hague. DOI: https://doi.org/10.1007/978-94-6265-285-9_4

Lloyd, I 2020 *Information Technology Law*. 9th ed. Oxford University Press. DOI: https://doi.org/10.1093/he/9780198830559.001.0001

Journals and Legal Analyses

Bartoszewicz-Rawlinson, A and **Given, P** 2021 EDPB's Guidelines on Territorial Scope – Clarifications and Uncertainties. *Privacy & Data Protection*, 20(4): 5–7.

Bellamy, J 2020 *An overview of FIFA's new data protection regulations*. [online] LawInSport. Available at: <https://www.lawinsport.com/topics/item/an-overview-of-fifa-s-new-data-protection-regulations> [Accessed 7 May 2021].

Blackshaw, I 2003 The Court of Arbitration for Sport: An International Forum for Settling Disputes Effectively 'Within the Family of Sport'. *Entertainment and Sports Law Journal*, 2(2): 4. DOI: https://doi.org/10.16997/eslj.139

Castro-Edwards, J 2021 Facebook, group litigation and distress: when will a precedent emerge? *Computers & Law*, Apr: 29–30.

Chapaneri, A 2020 Will this be the rise of UK privacy class actions? *Computer and Telecommunications Law Review*, 26(1): 1–2. DOI: https://doi.org/10.4324/9781003080510-1

Coleman, D and **Taylor QC, J** 2020 *Experts in the Hot Tub at the Court of Arbitration for Sport. Judicature*. Available at <https://judicature.duke.edu/articles/experts-in-the-hot-tub-at-the-court-of-arbitration-for-sport/> last accessed 9 May 2021.

De la Cruz, R 2020 Data protection contracts—what tends to be missing and what to do about it. *Privacy & Data Protection*, 20(8): 10–13.

Duval, A 2017 *Not in My Name! Claudia Pechstein and the Post-Consensual Foundations of the Court of Arbitration for Sport*. Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2017-01, Available at SSRN: https://ssrn.com/abstract=2920555. DOI: https://doi.org/10.2139/ssrn.2920555

Fierens, M and **de Bruyne, J** 2020 *Artificial intelligence in sports—the legal and ethical issues at play* – LawInSport. [online] LawInSport. Available at: <https://www.lawinsport.com/topics/item/artificial-intelligence-in-sports-the-legal-and-ethical-issues-at-play#_ftnref67> [Accessed 8 May 2021].

Flanagan, C 2020 *Manchester City's Financial Fair Play ban: the legal questions and consequences – LawInSport*. [online] Law in Sport. Available at: <https://www.lawinsport.com/topics/dispute-resolution/item/manchester-city-s-financial-fair-play-ban-the-legal-questions-and-consequences#_ftn3> [Accessed 23 April 2021].

Foster, K 2016 Lex Sportiva and Lex Ludica: the Court Of Arbitration for Sport's Jurisprudence. *Entertainment and Sports Law Journal*, 3(2): 2. DOI: https://doi.org/10.16997/eslj.112

Foster K 2019 Global Sports Law Revisited. *Entertainment and Sports Law Journal*, 17(1): 4. DOI: https://doi.org/10.16997/eslj.228

Gilchrist, W and **Phelops, W** 2017 *The legal implications for big data, sports analytics and player metrics under the GDPR – LawInSport*. [online] LawInSport. Available at: <https://www.lawinsport.com/topics/item/the-legal-implications-for-big-data-sports-analytics-and-player-metrics-under-the-gdpr> [Accessed 13 May 2021].

Greenbaum, D 2019 Wuz You Robbed? Concerns With Using Big Data Analytics in Sports. *The American Journal of Bioethics*, June 18(6). DOI: https://doi.org/10.1080/15265161.2018.1459953

Hasan, I 2020 Information commissioner gets busy with fines. [online] *Law Society Gazette*, 117(42): 21. Available at: <https://www.lawgazette.co.uk/legal-updates/information-commissioner-gets-busy-with-fines/5106553.article> [Accessed 5 May 2021].

Hessert, B 2020a Cooperation and reporting obligations in sports investigations. *International Sports Law Journal*, 20: 145–156. DOI: https://doi.org/10.1007/s40318-020-00169-5

Hessert, B 2020b Personal Real-time Sports Performance Information: Do Athletes Have a Say? *Jusletter*, 17 Fevrier 2020. DOI: https://doi.org/10.38023/c9144a5a-dd6b-444d-926f-24ee3c8cf1c3

Hopkins, R 2019 *Google and the emergence of opt-out data protection class actions*. [online] In-house Blog. Available at: <http://in-houseblog.practicallaw.com/google-and-the-emergence-of-opt-out-data-protection-class-actions/> [Accessed 5 May 2021].

Hutchins, B 2016 Tales of the Digital Sublime: Tracing the Relationship Between Big Data and Professional Sport. *Convergence: The International Journal of Research into New Media Technologies*, 22(5): 494–509. DOI: https://doi.org/10.1177/1354856515587163

Janeček, V 2020 Data protection, the value of privacy and compensable damage. *The Cambridge Law Journal*, 79(3): 417–420. DOI: https://doi.org/10.1017/S0008197320000719

Knight, C 2021 *GDPR and DPA 2018: claims for compensation*. [online] Practical Law. Available at: <https://uk.practicallaw.thomsonreuters.com/Document/Icb1e1dc2138b11e9a5b3e3d9e23d7429/View/FullText.html?transitionType=SearchItem&contextData=(sc.Search)&firstPage=true&comp=pluk#co_anchor_a729383> [Accessed 5 May 2021].

Kornbeck, J 2017 Athlete consent as a legal base for data transfers to third countries for anti-doping purposes, under EU and German law. *International Sports Law Journal*, 17: 68–85. DOI: https://doi.org/10.1007/s40318-017-0112-9

Kornbeck, J 2020 Statutory provision as a legal base for data transfers to third countries for anti-doping purposes, under EU and German law. *International Sports Law Journal*, 20: 55–81. DOI: https://doi.org/10.1007/s40318-019-00157-4

Novak, V and **Kühne, J P** 2020 *Health Data Transfer and Processing in CAS Proceedings*. CAS Bulletin, 2020/01. Lausanne. Available at: <https://www.tas-cas.org/fileadmin/user_upload/CAS_Bulletin_2020_1.pdf> [Last accessed 16 May 2021].

Oastler, K 2018 GDPR series: how to engage third party suppliers in a GDPR-compliant way. *Privacy & Data Protection*, 18(3): 3–6.

Patel, S and **Varley, I** 2019 Exploring the Regulation of Genetic Testing in Sport. *Entertainment and Sports Law Journal*, 17(5): 1–13. DOI: https://doi.org/10.16997/eslj.223

Rigozzi, A and **Quinn, B** 2014 *Evidentiary Issues Before CAS (May 19, 2014)*. Bernasconi, M (ed.), International Sports Law and Jurisprudence of the CAS – 4th Conference CAS & SAV/FSA Lausanne 2012, Editions Weblaw. Available at SSRN: https://ssrn.com/abstract=2438570

Roughton, A 2019 Damages in data protection cases – have the floodgates opened? *Privacy & Data Protection,* 20(1): 15–16.

Stalla-Bourdillon, S and **Knight, A** 2018 *Data analytics and the GDPR: friends or foes? A call for a dynamic approach to data protection law*. In R Leenes, R van Brakel, S Gutwirth, and P De Hert (Eds.), Data Protection and Privacy: The Internet of Bodies Hart. DOI: https://doi.org/10.5040/9781509926237.ch-011

Tran, D and **Adde, L** 2019 Joint controller relationships – more prevalent than previously thought? *Privacy & Data Protection*, 19(8): 6–8.

Viret, M 2019 *How Data Protection Crystallises Key Legal Challenges in Anti-Doping*. 7 May 2019, https://www.asser.nl/SportsLaw/Blog/post/how-data-protection-crystallises-key-legal-challenges-in-anti-doping-by-marjolaine-viret [Accessed 16 April 2021].

Waiting, M 2020 Top ten data protection considerations when outsourcing. *Privacy & Data Protection*, 20(7): 3–5.

Weatherill, S 2021 *Never let a good fiasco go to waste: why and how the governance of European football should be reformed after the demise of the 'SuperLeague'*. [online] Asser International Sports Law Blog. Available at: <https://www.asser.nl/SportsLaw/Blog/post/never-let-a-good-fiasco-go-to-waste-why-and-how-the-governance-of-european-football-should-be-reformed-after-the-demise-of-the-superleague-by-stephen-weatherill> [Accessed 7 May 2021].

Woods, L 2020 Schrems II. *Communications Law*, 25(4): 239–247.

Organisational publications/grey literature

EU Article 29 Working Party 2010 *Opinion 1/2010 on the concepts of "controller" and "processor"* (16 February 2010) Available at <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf> [accessed 26 April 2021].

European Commission 2021 *Adequacy Decisions*. [online] Available at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> [Accessed 28 April 2021].

European Union 2021 R*egulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. Available at <https://assets.contentstack.io/v3/assets/blt3de4d56151f717f2/bltcb14c2a9b8e72820/6086c50e26fd84453c019451/Draft_EU_AI_Regulation.pdf#page=23> [last accessed 8 May 2021].

European Data Protection Board 2020 *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.

FIFA 2019 *Data Protection Regulations*. [online] Available at <https://resources.fifa.com/image/upload/fifa-data-protection-regulations-2019.pdf?cloudid=dr9labmtd63ctx6o3erk> [Accessed 10 July 2020].

FIFA 2020a *Global Transfer Market Report 2020: A Review of International Football Transfers Worldwide*. Zurich: FIFA. Available at https://img.fifa.com/image/upload/ijiz9rtpkfnbhxwbqr70.pdf. Accessed 15 May 2021.

FIFA 2020b *FIFA Journal*. [online] FIFA Professional Football Journal. Available at: <https://www.professionalfootballjournal.fifa.com/> [Accessed 13 May 2021].

FIFPro 2020 *A Future Oriented Player Data Policy for the Digital Football Industry—The Collection, Protection, and Use of Player Data* [Online]. Available at <https://www.fifpro.org/media/31intkan/fifpro-policy-position_player-data_eng.pdf> [Accessed 12 May 2021].

ICO 2020a *Data Sharing Code of Practice*. Available at <https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf> [Accessed 27 April 2021].

ICO 2020b *Guidance on AI and Data Protection*. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/> [Accessed 8 May 2021.]

ICO 2021a *Legitimate interests*. [online] Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> [Accessed 16 April 2021].

ICO 2021b *What is special category data?* [online] Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd5> [Accessed 16 April 2021].

ICO 2021c *Right to be informed*. [online] Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/> [Accessed 13 May 2021].

ICO 2021d *Guide to Data Protection – What common issues might come up in practice?* [online] Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-common-issues-might-come-up-in-practice/> [Accessed 11 May 2021].

National Cyber Security Centre 2020 *The Cyber Threat to Sports Organisations*. [online] Available at <https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf> [Accessed 13 May 2021].

Premier League 2020 *Premier League Handbook Season 2020/2021*. Available at <https://resources.premierleague.com/premierleague/document/2021/03/24/20a9c091-be5a-4bf5-a9f4-87e2a86ad84f/2020-21-PL-Handbook-240321.pdf> [Last accessed 7 April 2021].

Websites

Collins, B 2021 *West Ham Utd Website Spills Supporters' Personal Data*. [online] Forbes. Available at <https://www.forbes.com/sites/barrycollins/2021/03/09/west-ham-utd-website-spews-out-supporters-personal-data/> [Accessed 23 April 2021].

Hynter, D 2014 *Arsenal's 'secret' signing: club buys £2m revolutionary data company*. [online] the Guardian. Available at <https://www.theguardian.com/football/2014/oct/17/arsenal-place-trust-arsene-wenger-army-statdna-data-analysts> [Accessed 21 April 2021].

Ornstein, D 2020 *Ornstein: Players to sue for hundreds of millions over use of their statistics*. [online] The Athletic. Available at <https://theathletic.co.uk/1949883/2020/07/27/ornstein-hundreds-players-lawsuit-southampton-leeds-wolves-premier-league/> [Accessed 8 March 2021].

Randall, C 2018 *StatsBomb Announces Free Data for Women's Football*. [online] StatsBomb. Available at <https://statsbomb.com/2018/06/statsbomb-announces-free-data-for-womens-football/> [Accessed 13 May 2021].

The Guardian 2020 *Manchester United hit by 'sophisticated' cyber attack but say fan data is safe*. [online] Available at <https://www.theguardian.com/football/2020/nov/20/manchester-united-confirm-cyber-attack-but-confident-match-can-go-ahead> [Accessed 23 April 2021].

Worville, T 2021 *Running Stats Explained: Pace, intensity and the Premier League 'plodders'*. [online] The Athletic. Available at: <https://theathletic.co.uk/2361681/2021/02/03/running-stats-pace-intensity-and-plodders-in-the-premier-league/> [Accessed 14 April 2021].

How to cite this article: Flanagan, CA. 2022. Stats Entertainment: The Legal and Regulatory Issues Arising from the Data Analytics Movement in Association Football. Part Two: Data Privacy, the Broader Legal Context, and Conclusions on the Legal Aspects of Data Analytics in Football. *Entertainment and Sports Law Journal*, 20: 1, pp. 1–16. DOI: https://doi.org/10.16997/eslj.1082

Submitted: 18 May 2021 **Accepted:** 17 August 2021 **Published:** 23 February 2022

Entertainment and Sports Law Journal is a peer-reviewed open access journal published by University of Westminster Press.

OPEN ACCESS