Nariat Pashaeva

Sui Generis Database Protection and Data-Sharing Obligations for Smart Balls in Football – Implications of the EU Data Act

Daten von vernetzten Sportgeräten werden im Profifussball zunehmend als wichtiger Wettbewerbsfaktor angesehen. Die EU-Datenverordnung verpflichtet die Hersteller intelligenter Produkte zum Teilen der Daten und kommt damit bestehenden Exklusivrechten in die Quere. Dieser Beitrag zeigt auf, wie Art. 43 der Datenverordnung das Schutzrecht sui generis von Datenbanken für maschinell erzeugte Sportdaten einschränkt und welche Konsequenzen dies für datenbasierte Geschäftsmodelle hat.

Les données issues des appareils de sport connectés sont de plus en plus considérées comme un facteur concurrentiel important dans le football professionnel. Le règlement européen sur les données oblige les fabricants de produits intelligents à partager les données, ce qui va à l'encontre des droits d'exclusivité existants. Le présent article montre comment l'art. 43 du règlement sur les données restreint le droit de protection sui generis des bases de données en ce qui concerne les données sportives générées automatiquement et quelles en sont les conséquences pour les modèles commerciaux basés sur les données.

Nariat Pashaeva, Cand.jur/JD (University of Oslo), LL.M. (University of Oslo), Associate Lawyer, Norway.

The english translation of the lead and summary is included on Swisslex and legalis only.

I. Introduction

1. Background and Scope

The increasing digitalization of the sports sector has led to a surge in the collection and use of data generated by connected products, such as «smart balls» in football. Connected products are electronic devices connected to the internet, commonly considered as part of the Internet of Things (IoT). In professional football, smart balls are used to collect real-time data on ball speed, trajectory, and spin, enabling coaches and analysts to enhance team performance, refine training methods, and make data-driven tactical decisions. These technological developments have brought complex legal questions to the forefront, concerning the ownership, access to, and protection of non-personal data.

With the application of the EU Data Act (Regulation 2023/2854) from September 2025, the regulatory landscape governing such data has shifted considerably. The Data Act introduces new rules on access to and sharing of data generated by connected products and related services. In doing so, it restricts the exercise of the *sui generis* database protection previously granted to database producers under the Database Directive. In particular, the ability of database producers to deny access to non-personal data obtained from or generated by connected products has been narrowed.

This article explores the implications of these new rules by analysing how Art. 43 of the Data Act, read in conjunction with Art. 4, limits the scope of *sui generis* database protection in the context of the sports industry. The *sui generis* right is a form of protection granted to database producers

in recognition of their investment in the obtaining, verification or presentation of a database.[1] While this right formally remains in force, its practical reach is increasingly constrained by the data access and sharing obligations introduced by the Data Act.

This analysis is anchored in a hypothetical business-to-business relationship, in which a professional football club (FairPlay FC) contracts with a technology provider for smart balls (SB Technologies) and an associated analytics application. Data generated by smart balls is transmitted to the provider's platform, where it is stored, organized, and potentially combined with other datasets to create additional value. The structure and management of these data flows are central to determining legal rights and obligations of the parties.

After having relied on this system, to optimise training and performance, the FairPlay FC seeks to switch providers and requests access to its historical data. This scenario raises the central legal question examined in this article: which categories of data – raw, pre-processed, and derived or inferred – must be made available to the football club under the Data Act, and under what conditions may database protection still be invoked. The analysis therefore focuses on data access obligations before data are made available to the user.

Methodologically, the article employs a doctrinal legal and interpretative approach grounded in the text of the Data Act and the Database Directive with relevant case law of the Court of Justice of the European Union (CJEU). In the absence of established case law interpreting the Data Act, the analysis is supplemented by academic commentary and official reports. The article is complemented by a limited comparative perspective, with reference to Swiss law. The scope of the article is limited to non-personal, commercial data, while personal data and mixed datasets are expressly excluded.

This article argues that, in contexts governed by the EU Data Act, the practical effect of Art. 43 is to significantly weaken the exclusivity traditionally afforded by the *sui generis* database right, particularly in relation to machine-generated data produced by smart devices.

2. The Data Economy, Smart Balls and Data Generation in Football

The European Commission estimates that approximately 80% of industrial data remains unused.[2] The Data Act responds to the EU's and the market's increasing need to exploit data, so that the data economy can be realised. In order to make better use of industrial data, the Regulation determines «who can use data to create something of value, and under which conditions».[3] To develop and promote a competitive data economy, the Regulation grants users of connected products and related services access to data generated through purchase, rental, or leasing.[4]

IoT products generate data in the course of normal use, and it is precisely this data generation that constitutes a core part of their value.[5] A connected product is an item that obtains, generates, or collects data concerning its use or environment and that is able to communicate product data via an alectronic communications service, physical connection or on-device-access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user.[6]

A related service is a digital service that is connected to the connected product in such a manner that, in its absence, the connected product would be prevented from performing one or more of its functions.[7] Such services may include applications that allow users to interpret data generated by the connected product, provided that they do not qualify as electronic communications services. The technology provider typically qualifies as both the database producer and the data holder, while a football club qualifies as the user within the meaning of the Data Act.

The sports sector is increasingly shaped by digital technologies and the growing importance of data-driven decision-making. Connected products and analytics platforms are transforming how sports clubs, leagues, and technology providers operate, creating new opportunities as well as legal challenges. Today, a significant majority of professional sports teams, approximately 75%, rely on real-time analytics to enhance team performance,[8] and the sports analytics market is forecast to grow from USD 5.79 billion to USD 24.03 billion by 2032.[9]

Smart balls equipped with sensors generate large volumes of non-personal data, with little to no human interaction. These devices capture real-time data that are transmitted to the cloud and stored in databases, where they are processed and presented to the football club through an application. The data may include information on speed, spin, and trajectory, which the football club uses to inform training and tactical decisions. The integration of such technology exemplifies the shift toward a data-centric approach in professional football.

1 Article 7 of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27 March 1996, 20–28.

2 European Commission, «Data Act: Commission proposes measures for a fair and innovative data economy», ‹ec.europa.eu/commission/presscorner/detail/en/ip_22_1113› (January 2026).

3 European Commission, «Data Act explained», ‹digital-strategy.ec.europa.eu/en/factpages/data-act-explained› (January 2026).

4 European Commission (n. 3).

5 European Commission «Data Act», ‹digital-strategy.ec.europa.eu/en/policies/data-act› (January 2026).

6 Article 2(5) of the Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394; Directive (EU) 2020/1828 (Data Act), OJ L 2023/2854, 22 December 2023.

7 A related service may be added later with the aim of adapting, adding to, or updating the functions of the connected product. See Article 2 (6) EU Data Act.

8 S. Sristava, «The Business Opportunities and Challenges of Implementing Analytics in Sports», ‹appinventiv.com/blog/data-analytics-in-sports-industry/› (January 2026).

9 S. Srivstava (n. 8).

The legal landscape governing sports data is evolving, with particular attention to the interaction between exclusive database protection and mandatory data access obligations. Understanding how the Data Act reshapes the balance between database producers and users is essential for stakeholders operating in data-driven sports markets, where access to historical and real-time data may determine competitive advantage.

II. Legal Framework

1. The EU Data Act and the Data Economy

The EU Data Act introduces new rules on data access and sharing, specifically targeting data generated by connected products, while the Database Directive establishes *sui generis* protection for databases. Data are often referred to as the new oil, and they can also be used to render a company competitive in a market; however, data, much like oil, must be processed before any value can be extracted. This can be explained by a quotation from Siemens: «We need to understand that data is everywhere and that it is generated every second of the day. We need to understand data as an asset and turn it into a value».[10] The Data Act pursues several different objectives, one of the main ones being to develop the data economy.[11] Another objective is to rebalance control over data by shifting certain powers from data holders and other commercial actors to users. This reallocation of control affects the commercial actors that design, supply, and monetise connected products and related services.

Both the data economy and the digital economy are mentioned in the Data Act, but neither concept is defined. The data economy focuses on data sharing and value creation. To achieve effective markets for non-personal data, it is important that users of connected products are also able to share data with others without encountering major technical obstacles. The data economy cannot be realized without circulation. The digital economy focuses on the market as a whole, on breaking up monopolies, and, more generally, ensuring harmony in the internal markets. The data economy, on the other hand, focuses on access to data and how data can generate value. There is no rigid boundary between the two. In the literature and in other reports, the terms digital economy and data economy are often used interchangeably.[12]

a) Data under the Data Act

The distinction between raw, processed, derived, and inferred data is central to the functioning of the Data Act, as it determines both the scope of data access obligations and the relevance of database protection. In the Data Act, data is defined as «any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording».[13] It is therefore clear that the concept of data is broad. Both data from connected products and data from related services are regulated by the Data Act. This applies to data generated «directly» and «indirectly» through the use of these products or related services, and even when the user is not actively using the product.[14]

Raw and processed data are addressed in the recitals in the Data Act. Raw data is defined as primary or source data, that is, data which have not been processed and which originates directly from the source.[15] Processed data is data that have been processed in order to present the information in a «useable» or «understandable» manner.[16] Regarding the latter, the Data Act clarifies that such processing does not involve «substantial investments», which, is a condition for obtaining *sui generis* protection. The Regulation does not further define the content of raw and processed data. However, the purpose of the qualitative requirements imposed by the Data Act, appears to be ensuring that the user can access and use the data without expending undue effort.[17]

Information that is inferred or derived from data falls outside the scope of the Regulation.[18] This is explained by the fact that such data result from additional investments in order to obtain insights from the data or to assign values to them. Proprietary, complex algorithms are mentioned in particular in this context. Inferred and derived data are likewise not subject to the data-sharing obligation.

The Regulation does not further specify where the boundary lies between raw or processed data, on the one hand, and inferred or derived data, on the other. It should be emphasised that a user's right of access to data generated by a connected product is not the same as obtaining database rights.

10 Siemens Knowledge Hub. Siemens Smart data. [Video] ‹www.youtube.com/watch?v=ZxoO-DvHQRw› (January 2026); On data's competitiveness in the market see, A. Aridu/U. Petrovcic, Big Tech, Small Tech, and the Data Economy: What Role for EU Competition Law?, World Bank Group, Washington 2019, 26.

11 Recitals 32 and 119, Data Act.

12 A. Aridu/U. Petrovcic at World Bank Group refer to the ‹data economy› while relying on sources that use the term «digital economy» (n. 10). In particular they refer to United Nations Conference on Trade and Development (UNCTAD), Competition issues in the digital economy, Note by the UNCTAD secretariat, TD/B/C.I/CLP/54, 1 May 2019.

13 Article 2(1) Data Act. The Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to an use of data (Data Act), COM/2022/68 final contained the same definition, see Article 2(1).

14 Recital 15 Data Act. Emphasis added.

15 Recital 15 Data Act.

16 Recital 15 Data Act.

17 These qualitative requirements are examined more in detail in section III. Although third parties fall outside the scope of this article, the requirements that data be «usable» and «understandable» apply equally to them. See further European Commission, *Frequently Asked Questions – Data Act*, Version 1.2, 3 February 2025, 7 ‹www.dirittobancario.it/wp-content/uploads/2025/02/FAQs-Commissione-UE-03-febraio-2025-versione-1.2.pdf› (January 2026); On «usability» as a parameter under the Data Act, see D. Kim/M.W. Kwok, Data useability as a parameter of rights and obligations under the EU Data Act, JIPITEC 2024, 139 ff., who argue that usability has not been sufficiently addressed in the Regulation.

18 Recital 15 Data Act.

2. The Database Directive

a) Purpose, rationale and sui generis protection

The purpose of the Database Directive is not to protect data as such, but to protect the database that is formed by various data. A database is a «collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means».[19] According to its wording, this definition covers both electronic and non-electronic databases. The definition is broad,[20] but there are nonetheless no indications in the wording suggesting that machine-generated data automatically fall within this definition. Furthermore, one may ask how far the requirement of being «independent» extends. The fact that it is mentioned first, and only once, may indicate that the subsequent «data» and «materials» must also meet the same level of independence. The definition is general and says nothing more about the producer or author.

Since its introduction in 1996, the *sui generis* database right has been subject to sustained criticism. Concerns have focused on its conceptual uncertainty,[21] its impact on competition, and its limited contribution to the development of data-driven economy.[22] Both the European Commission and the European Parliament have questioned whether the Database Directive has achieved its stated objectives.[23]

Databases may enjoy two different forms of protection under EU law, reflecting a so-called «two-track system». This system is not unique to databases and can also be recognised in the protection afforded to photographs; while this article focuses on limitations to the *sui generis* right under the Data Act, it also briefly considers why copyright remains exempt. Whereas *the sui generis* database right rewards substantial investment in the obtaining, verification, or presentation,[24] copyright is reserved for databases that constitute the author's own «intellectual creation».[25] This reflects the central role of originality in copyright protection.[26]

Both the Database Directive and the Data Act pursue different objectives, but they converge in that both seek to stimulate innovation. It is difficult to promote competition when large actors enjoy a monopoly over certain types of data – the Data Act is an attempt to redistribute data in the market.

Article 7(1) of the Database Directive lays down the conditions for obtaining protection («substantial investment») and the scope of protection once it has been obtained («extraction» and «re-utilisation»). In the following, the conditions for obtaining *sui generis* protection are examined first, followed by an analysis of the scope of that protection. *Sui generis* database protection does not presuppose human authorship. It suffices that a company has invested in the database, meaning that the company takes the initiative and bears the risks associated with investing in the database.[27] Subcontractors do not fall within this protection.[28] Identifying the database producer may prove difficult, particularly in cases involving several investors.[29]

b) Conditions for obtaining protection

The conditions for obtaining *sui generis* database protection have been clarified primarily through CJEU case law. The Court has consistently emphasised that the decisive factor is not the investment made in generating the underlying data, but the investment directed at obtaining, verifying, or presenting those data as database contents. Accordingly, investments in data creation do not attract *sui generis* protection.

In *British Horseracing Board* (C-203/02), the Court held that «obtaining» refers to the resources used to seek out existing independent materials and collect them into a database.[30] By contrast, resources devoted to creating the data («materials») that constitute the contents of the database fall outside the scope of protection. The same logic applies to «verification», which encompasses resources used to ensure the reliability of the database contents («information»), both at the time of its creation and during its operation. Monitoring activities carried out at the stage of data crea-

19 Article 1(2) Database Directive; See also Article 10(2) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), Annex 1c to the Marrakesh Agreement Establishing the World Trade Organization of 15 April 1994, 1869 UNTS 299, which defines databases as «[c]ompilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such».

20 This has been acknowledged in the literature; see, for example, J.D. LIPTON, Wikipedia and the European Union Database Directive, Santa Clara Computer & High Technology Law Journal 2010, 631 ff, and R. Fisher/J. Chicot/A. Domini/M. Misojcic/G. Bodea/K. Karanikolova/A. Radauer/A. Gkogka/M. del C. Calatrava Moreno, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, Final Report, study prepared for the European Commission by Joint Institute for Innovation Policy and Technopolis Group, 2018.

21 Distinguishing the *sui generis* right from copyright was also a further step in complicating these forms of protection because the dual track has «caused confusion among users as the same database can be protected by both copyright and ‹sui generis› right». This prevented users from even attempting to use databases, either out of pure confusion or because they feared infringing database holders' rights, cf. COMMUNIA Association, *Policy Paper in reaction to the public consultation on the Database Directive*, August 2017, 2–3.

22 European Parliament, *Towards a Digital Single Market Act*, A8-0371/2015, 2015 para. 108.

23 See Commission of the European Communities, DG Internal Market and Services, Working Paper, *First evaluation of Directive 96/9/EC on the legal protection of databases*, Brussels, 12 December 2005, 1 ff., finding that the conditions in Article 7 lack precise legal meaning and that the effects of the *sui generis* right are difficult to assess. Similar concerns were raised in the 2018 evaluation Fisher/Chicot/Domini/Misojcic/Bodea/Karanikolova/Radauer/Gkogka/Moreno (n. 20), ii-iii, noting that the economic justification for the *sui generis* right remains highly contested; See also *Commission Staff Working Document – Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, Brussels, 25 April 2018.

24 Article 7 Database Directive.

25 Article 3 Database Directive.

26 Swiss law does not recognise an autonomous *sui generis* database right. Database protection is available only where the requirements of originality under copyright law are met. See section III.5.b) below.

27 Recital 41 Database Directive.

28 Recital 41 Database Directive.

29 O.A. ROGNSTAD, Opphavsrett, 3rd edition, Oslo 2019, 393.

30 ECJ of 9 November 2004, C-203/02, «BHB v. William Hill», paras 31, 42.

tion, which become part of the database, are likewise excluded. «Presentation» concerns investments made in organising and displaying the contents of the database in a systematic or methodical manner.

The requirement of «substantial investment» encompasses both qualitative and quantitative investments. Qualitative investment may include the deployment of specialised expertise or technical know-how, while quantitative investment refers to financial resources, labour, or time devoted to the database.[31]

Sui generis protection lasts for 15 years from the completion of the database.[32] This limited duration may, however, be effectively extended where the database owner makes a «substantial investment». The possibility of repeated renewal has raised concerns that databases may, in practice, remain protected indefinitely, thereby preventing their contents from entering the public domain. Unlike copyright works, such as books and photographs, which enter the public domain 70 years after the author's death. Perpetual renewal of database protection has been described as «a fundamental threat» to the information commons.[33]

c) Scope of Protection

For databases that enjoy *sui generis* protection, extraction or reutilization of all or a substantial part of the database may not be carried out without the owner's consent. The scope of the protection has been interpreted broadly in several cases, but in *Melons* (C-762/19), which concerned a search engine for job advertisements, the Court introduced a balancing of interests.[34]

The terms «extraction» and «re-utilization» are defined in law. «Extraction» is understood as the «permanent or temporary transfer of all or a substantial part of the content of a database to another medium by any means or in any form»,[35] while «re-utilization» covers «any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, renting, by on-line or other forms of transmission».[36] The wording of the provisions illustrates that, in light of existing case law, legal definitions alone are insufficient, a conclusion that emerged both in the 2005 and the 2018 evaluations of the Database Directive.[37]

In *Freistaat Bayern* (C-490/14), referring to *Fixtures Marketing* (C-444/02), the CJEU further clarified that the assessment of unlawful extraction or re-utilisation does not depend solely on the value of the data for the database maker. Materials that are of limited value to the maker may nonetheless be of significant value to third parties.[38]

In *Melons* (C-762/19), the CJEU examined whether hyperlinks, redirecting users to the database owner's website constituted re-utilization, and whether the display of metatags amounted to extraction.[39] The autonomy and choices of the database owner were taken into account, since the possibility of «exploring» several databases was a consequence of the data having been made publicly available, «since anyone at all can use a search engine».[40]

Transferring the contents of a database to another platform without consent qualifies as extraction or re-utilisation when it has «the effect of depriving» the database maker «of income intended to enable him or her to redeem the cost of that investment».[41] In this assessment, the Court emphasised the risk of producing a parasitical competing product and focused on whether the interference threatened the database maker's ability to harvest the fruits of the substantial investment.[42]

The introduction of this additional assessment marked a departure from earlier case law, which had interpreted the *sui generis* right expansively.[43] Husovec and Derclayce describe this as «a different flavour»,[44] and van Eechoud has characterised the additional condition as a «harm-based» threshold.[45] By introducing this additional condition, the CJEU has complicated «the coherent application of the qualitative/quantitative criterion to both investment (…) and extraction/re-use (…)».[46]

It is noteworthy that in the *Melons* judgment, the CJEU did not address the requirement that database contents be «individually accessible» within the meaning of Art. 1(2) of the Database Directive. In practice, hyperlinks may render individual elements accessible to end users, raising ques-

31 See, *inter alia*, the 2018 Evaluation of the Database Directive, p. 8, noting the lack of clarity regarding the level of time and financial investment required to satisfy the threshold of substantial investment.
32 Article 10(1) Database Directive.
33 COMMUNIA (n. 32), 2.
34 See ECJ of 8 June 2004, C-203/02, «*BHB v William Hill*», paras. 51–53; EJC of 9 October 2008, «*Directmedia*», paras. 31–33; ECJ of 5 March 2009, C-545/07, «Apis», para. 40; ECJ of 19 December 2013, C-202/12, «*Innoweb*», paras. 33–34, 38; ECJ of 3 June 2021, C-762/19, «*CV-Online*».
35 Article 7(2)(a) Database Directive.
36 Article 7(2)(b) Database Directive.
37 Commission of the European Communities (n. 23) and European Commission (n. 20).
38 Cited in ECJ of 29 October 2015, C-490/14, *Freistaat Bayern v Verlag Esterbauer GmbH*, para. 27; ECJ of 9 November 2004, C-444/02, «*Fixtures Marketing*», para. 34.
39 C-762/19 para. 15; The essence of the questions are paraphrased.
40 C-762/19 para. 35 and C-202/12 para. 51; Making data available to the public triggers «re-utilization» within the meaning of the Database Directive, cf. Art. 7(2)(b).
41 The fact that CV-Online itself had included the relevant metatags in the website design was of «secondary importance», as the decisive element was that Melons had engaged in extraction and re-utilization without consent, see C-762/19 para. 37; See also the Opinion of Advocate General Szpunar, para. 36.
42 C-762/19, paras 38–41; C-202/12 «*Innoweb*», para. 48 (n. 44); Recitals 39 and 43 of the Database Directive. See also the Opinion of Advocate General Szpunar, paras. 39 et seq.
43 M. van Eechoud, Database Rights in the EU's Data Strategy: A Question of Sport?, Intellectual Property and Sports: Essays in Honour of P. Bernt Haugenholtz, Information Law Series 2021, 258.
44 E. Derclaye/M. Husovec, «Access to information and competition concerns enter the sui generis right's infringement test – The CJEU redefines the database right», *Kluwer Copyright Blog*, 17 June 2021, ‹copyrightblog.kluweriplaw.com/2021/06/17/access-to-information-and-competition-concerns-enter-the-sui-generis-rights-infringement-test-the-cjeu-redefines-the-database-right/›; Derclaye was also one of the two appointed experts in the European Commission's 2018 evaluation of the Database Directive (n. 20).
45 van Eechoud (n. 43), 258.
46 van Eechoud (n. 43), 258.

tions as to how broadly this criterion should be interpreted. While a permissive interpretation could have far reaching implications, this issue falls outside the scope of the present analysis. Although not relevant to this contribution, there are some exceptions to the *sui generis* right found in the Database Directive Art. 9(1).

The foregoing analysis demonstrates that the *sui generis* right under the Database Directive is conceptually broad, yet marked by persistent uncertainty with respect to its scope. These ambiguities form the point of departure for assessing the impact of the EU Data Act, and in particular Art. 43, on the continued relevance and operation of database protection. This assessment is especially pertinent in data-sharing contexts involving machine-generated data and data-driven sports environments.

III. Data Sharing and Sui Generis Protection for Smart Sports Devices Under the Data Act

1. Introduction

When proposed, Art. 35 (now adopted as Art. 43) attracted criticism for its ambiguous wording and its potentially far-reaching consequences concerning database protection. The changes made during the legislative process are therefore relevant for understanding the scope and limits of the final provision.

This section compares the wording of adopted Art. 43 with that of proposed Art. 35 in order to identify whether, and to what extent, the legislator sought to clarify, narrow, or expand the limitation of the *sui generis* right. This comparison provides the interpretive backdrop for the subsequent analysis of machine-generated data under the Database Directive (section 3) and the data access obligations under Art. 4 of the Data Act (section 4).

2. Adopted Art. 43 and Proposed Art. 35

Article 43 is shorter than proposed Art. 35, indicating a more precise wording. Article 35 introduced the purpose of the provision in its first sentence and explained that the provision was necessary in order not to hinder users' access to and use of data.[47] The adopted Art. 43 does not contain such wording. It may be that this clarification was considered superfluous, since the recitals already make clear that the legislator seeks to facilitate the free flow of data for users, including both consumers and commercial actors.[48]

Article 35 stated that the provision was to be interpreted «in accordance with Article 4» and «Article 5», which has now been replaced by «in particular in relation to Articles 4 and 5 thereof». This indicates that Art. 43 is not limited to Arts. 4 and 5, but may also apply to other provisions of the Data Act.

Proposed Art. 35 limited the *sui generis* right for databases containing data «obtained from or generated by the use of a product or a related service».[49] By contrast, the adopted Art. 43 applied the limitation to data «obtained from or generated by a connected product or related service falling within the scope of this Regulation». The shift from «use of product or a related service» to data generated by a «connected product or related service» suggests a shift from user activity to the technical characteristics and regulatory scope of the product itself. The addition of the phrase «falling within the scope of this Regulation», further ties the limitation to the material scope of the Data Act, a point that becomes decisive for historical and training data.

One criticism levelled at the proposed Art. 35 was that databases falling within its scope would no longer be regulated by any other legislation.[50] Although the wording of Art. 43 has been amended, this concern has not been fully resolved. In particular, the reference to Art. 43 applying «in particular» in relation to Arts. 4 and 5 leaves open whether the limitation of the *sui generis* right may also influence the interpretation of other provisions of the Data Act. As a result, the precise reach of Art. 43, and its interaction with the Database Directive, remains uncertain.

Whereas Art. 35 expressly stated that the *sui generis* right «does not apply» to certain databases, the adopted Art. 43 provides that the *sui generis* right «shall not apply». This may be a deliberate change in wording, which could suggest that there are exceptional cases falling outside Art. 43 and left to the Member States to interpret, but according to the EU's Style Guide, «shall» is to be understood as «must» in EU legislation.[51]

Building on these textual changes, two key differences can be identified. First, data that have not been obtained or generated through use, may also fall within the scope of Art. 43.[52] Second, Art. 43 specifies that protection is limited to data falling within the scope of the Data Act, meaning derived and inferred data, which are results of additional investments, are not affected by Art. 43. These changes illustrate that the limitation of the *sui generis* right is no longer confined to situation governed exclusively by Arts. 4 and 5. The use of the phrase «in particular» leaves open whether Art. 43 interpreted in conjunction with Arts. 4 and 5, will be more narrow than other provisions that are not expressly mentioned. The scope of Art. 43 therefore remains unclear.

Under proposed Art. 35, databases containing data generated during training would likely fall outside *sui generis* protection, meaning SB Technologies would probably have to grant access to FairPlay FC. The adopted Art. 43

47 Article 35 proposed Data Act.
48 See Recitals 5, 68 and 119.
49 Article 35 proposed Data Act.
50 M. Husovec/E. Derclaye, Why the sui generis database clause in the Data Act is counter-productive and how to improve it?, SSNR 2022, 2–3. Since the Data Act did not explicitly preclude Member States from regulating this at national level, the proposed provision raised concerns that regulatory gaps or divergent national interpretations could emerge.
51 European Commission, *English Style Guide: A handbook for authors and translators in the European Commission*, 8th edn. of January 2016 (last updated August 2025), notes 10.25 and 10.28; For a discussion of the normative force of ‹shall›, see A. Felici, ‹Shall› Ambiguities in EU Legislation, Comparative legilinguistics 2012, 51 ff.
52 Passive use falls within the Data Act, see recitals 15 and 35.

shifts the focus to whether the data are obtained from or generated by a connected product within the scope of the Data Act, creating uncertainty about the continued applicability of database protection for historical match and training data.

3. The Relevance of the Sui Generis Right For Machine-Generated Sports Data

A connected product is defined in the Data Act as a product that «obtains, generates and collects data»,[53] whereas Art. 43 limits the *sui generis* right only in respect of data «obtained from or generated by» a connected product. The omission of «collects» from Art. 43 is therefore notable.

Several explanations may account for this divergence. One possibility is that the mere collection of machine-generated data was not considered sufficient, in itself, to satisfy the requirement of substantial investment under the Database Directive. Another possibility is that the legislature implicitly regarded the collection of data as subsumed under the notion of generation, although this does not fully explain why «collects» is explicitly included in the definition of a connected product. A third, less plausible, possibility is that the distinction between collecting and generating data was regarded as too indeterminate to function as a legal criterion.

Another explanation may be found in the Commissions' observation that databases increasingly contain a mixture of machine-generated and human-generated data, and that such databases should not automatically fall within the scope of *sui generis* protection.[54] This approach may be intended to incentivize the development of technologies capable of distinguishing between different categories of data within complex datasets.[55]

More convincingly, however, the omission of «collects» can be understood as reflecting an intention to preserve the *sui generis* right for data for which the database maker has made additional investments. According to this reading, «collects» refers to data that fall outside the scope of Art. 43, such as derived or inferred data, which the Data Act expressly excluded from mandatory sharing. This interpretation aligns with the logic of the Database Directive under which protection attaches not to the creation of data as such, but to substantial investment in their collection, verification or presentation.

Chapter II established that databases which do not qualify for *sui generis* protection are likewise not protected against extraction or re-utilization under Art. 7 of the Database Directive. Against this background, Art. 43 of the Data Act may, albeit implicitly, modify the practical reach of the protection afforded by the Database Directive. Whether this creates a legal vacuum is uncertain.

The relevance of the *sui generis* right for machine-generated sports data depends not only on the wording of Art. 43, but also on how the concepts of «obtaining», «generating», and «collecting» data, are understood in relation to connected products. This question is particularly salient in the context of IoT technologies, which generate large volumes of data as a by-product of their primary functions.[56]

The Commission has consistently expressed scepticism as to whether the *sui generis* right provides meaningful incentives for the creation of databases containing machine-generated data.[57] In the impact assessment accompanying the Data Act, the Commission concluded that the *sui generis* right has little or no positive effect on database creation, especially where data are generated incidentally to other economies activities.[58] At the same time, the Commission acknowledged that excluding machine-generated data from the scope of the Database Directive would require legislative clarification, suggesting that their current legal status cannot be regarded as settled.[59]

This ambivalence is also reflected in earlier Commission documents, which state both that the *sui generis* right «does not apply to machine-generated data as such»[60] and that it remains unclear whether such data fall within the definition of a database or should benefit from protection.[61] Stakeholder views are similarly divided. While a majority of respondents to the 2018 evaluation considered exclusion beneficial for research and innovation,[62] a significant proportion of database makers reported that the *sui generis* right encouraged investment in advanced information systems.[63]

National case law further illustrates this uncertainty. In Germany, courts have recognised *sui generis* protection for databases composed of machine-generated data, notably in the *Autobahnmaut* case, where toll-collection data were found to be systematically arranged and thus capable of protection.[64] The Commission has also acknowledged that some stakeholders consider the *sui generis* right to already extend to machine-generated data, although this position has not been substantiated in detail.[65]

These ambiguities form the background against which Art. 43 must be understood. The impact assessment underpinning the Data Act identified an imbalance in data shar-

53 Article 2(5) Data Act.
54 A. Wiebe, *Study to Support an Impact Assessment for the Review of the Database Directive, Copenhagen Economics*, European Commission, Directorate-General for Communications Networks, Content and Technology, Luxembourg 2022, 67.
55 Wiebe (n. 54).
56 European Commission, Commission Staff Working Document – Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)», SWD(2022) 34 final, Brussels, 23 February 2022 (accompanying COM(2022) 68 final; SEC(2022) 81 final; SWD(2022) 35 final, 15.
57 SWD(2022) 34 final (n. 56), 137.
58 SWD(2022) 34 final (n. 56), 137–138.
59 SWD(2022) 34 final (n. 56), 45.
60 European Commission, *Commission Staff Working Document – On the free flow of data and emerging issues of the European data economy*, SWD (2017) 2 final, Brussels, 10 January 2017 (accompanying COM (2017) 9 final, 20.
61 Fisher/Chicot/Domini/Misojcic/Bodea/Karanikolova/Radauer/Gkogka/Moreno (n. 20), 1 ff.
62 SWD(2022) 34 final (n. 56), 16.
63 SWD(2018) 146 final (n. 23), 17.
64 BGH of 25 March 2010, I ZR 47/08, «*Autobahnmaut*», para. 13.
65 SWD(2022) 34 final (n. 56), 136.

ing between data holders and users, and noted that data holders might otherwise benefit from an expansion of the *sui generis* right.[66] Article 43 therefore appears to function as a precautionary provision, particularly as the economic value of such data continues to increase.

Despite the adoption of Art. 43, significant legal uncertainty remains as to the precise boundary between protected database investments and data subject to mandatory access obligations under the Data Act. In particular, the absence of clear definitions of ‹machine-generated data› and the continued indeterminacy of concepts such as ‹substantial investment› leave considerable discretion to courts and, potentially, to national legislators. Until further judicial clarification emerges, the interpretation of Art. 43 will therefore require careful balancing between the objectives of incentivising data-driven investment and promoting access to and re-use of data.

By limiting reliance on the *sui generis* right in defined circumstances, Art. 43 is expected to reduce transaction costs, facilitate access to and use of data, and curb opportunistic litigation.[67] In this sense, the provision operates as a regulatory steering mechanism in an unresolved legal landscape, aligning the objective of the Data Act with the competition-oriented rationale that also underpinned the Database Directive.[68]

a) Collecting or generating data through smart balls

This subsection examines when data generated by a connected product, specifically a sensor-based smart football, may constitute a database protected by the *sui generis* right, and consequently when Art. 43 of the Data Act applies. The analysis focuses on the legal characterisation of the data, rather than on the underlying technical processes.

The Data Act does not abolish the *sui generis* right as such but limits its applicability to databases containing data obtained or generated by connected products or related services. Applied to SB Technologies, the key question is therefore whether the smart ball collects existing data or generates new data. This distinction remains contested at the EU level,[69] as reflected in the 2018 evaluation report, which noted the increasing difficulty of distinguishing between data creation and data obtaining when there is systematic categorisation of data already by the data-collecting object.[70]

A sensor-based smart ball does not create speed, spin, or trajectory. It measures these physical phenomena that already exist. As with meteorological measurements, such data are collected, verified or presented rather than created.[71] Investments in recording existing phenomena are therefore more plausibly characterised as investments in collecting data, which may fall within Art. 7, than as investments in creating data, which do not. While opinions diverge, there are stronger doctrinal indications that investments in systematic measurement and recording satisfy the concept of «obtaining» data within the meaning of the Database Directive.[72]

Once collected, the data must be processed to become useable. Where SB Technologies invests substantially in the verification or presentation of these data, whether in terms of financial resources, time, or specialised expertise, such investments may satisfy the conditions for *sui generis* protection, even if the initial data acquisition is automated. The mere fact that data are obtained automatically is therefore not, in itself, decisive.

For the purposes of the Data Act, the decisive criterion is the degree of data enrichment.[73] Data originating directly from sensors, together with associated metadata, constitute raw or pre-processed data and fall within the scope of the Regulation. This includes measurements of speed, spin, and trajectory generated by the smart ball.[74] Pre-processing should not be understood as requiring substantial investments in cleaning or transformation, rather, it refers to minimal processing necessary to render the data useable.[75] The threshold between expected processing, on the one hand, and enrichment requiring substantial investment, on the other hand, must be assessed on a case-by-case basis.

By contrast, enriched data, such as inferred or derived data resulting from additional analytical investments, fall outside the scope of the Data Act. Derived data typically involve relatively simple calculations, such as aggregated performance metrics,[76] whereas inferred data are probability-based and result from more complex analyses, such as predictive or tactical assessments.[77] These forms of second-generation data provide an indicative benchmark for the level of investment capable of satisfying the requirement of «substantial investment» under the Database Directive.

Read in light of recent case law, including *Melons*, Art. 43 reflects a broader policy shift towards limiting the scope of database protection where competing interests, such as access to data and market competition, are at stake.[78] In the context of the data economy, an increasing number of databases may therefore fall outside the scope of *sui generis* protection.

Applied to SB Technologies, this development does not appear disproportionate. While raw and pre-processed data generated by the smart ball must be made available to Fair-

66 SWD(2022) 34 final (n. 56), 134.
67 SWD(2022) 34 final (n. 56). 136.
68 SWD(2018) 146 final (n. 23), 12.
69 Fisher/Chicot/Domini/Misojcic/Bodea/Karanikolova/Radauer/Gkogka/Moreno (n. 20) vi.
70 See European Commission «Study to Support» (2022), (n. 54) 55, and SWD(2018) 146 final (n. 23), 15.
71 O.A. Rognstad (n. 29), 396.
72 O.A. Rognstad (n. 29), 396 for a general discussion and further references on the concept of «obtaining».
73 European Commission (n. 17), 6.
74 European Commission (n. 17), 6.
75 Recital 15 Data Act.
76 D. Abecassis/R. Morgan, *The use of data by online services*, Consulting report for Ofcom, Analysys Mason, London, May 2019, 6–7.
77 Z. Khan, The Integration of Internet of Things (IoT) in Precision Agriculture, Agricultural and Biological Research 2024, 1194–1195.
78 Such a development would align with arguments advanced by COMMUNIA, which has argued that the renewable 15-year protection period negatively affects the information commons, see n. 32.

Play FC pursuant to Art. 43, SB Technologies retains control over enriched data resulting from additional investments. This allocation reflects the balancing of interests underlying the Data Act.

4. Article 4: Data-Access Obligations in Professional Football

a) Introduction

Section 3 examined how Art. 43 of the Data Act limits the applicability of the *sui generis* database right in respect of data obtained from or generated by connected product or related service. The present section turns to Art. 4 and analyses how the data access obligations, imposed on data holders, operationalise that limitation in practice.

Article 4 governs the circumstances under which users may request access to data and the conditions under which such access must be granted. Read in conjunction with Art. 43, it further constrains the ability of database producers to rely on exclusive rights to restrict access to machine-generated data.

Sections (b)-(e) address key aspects of the Data Act's obligations and limitations: (b) the data holder's sharing obligations, (c) the limitations on circumventing Art. 4, (d) exceptions to the data-sharing obligation, and (e) restrictions on users after data have been made available.

b) Data holder's data-sharing obligations vis-à-vis football clubs

Article 4 applies when a user requests access to data generated by a connected product or related service. Under Art. 3(1), the manufacturer must design and produce products and services so that data are, where technically possible, «directly accessible».[79] Article 4(1) applies where such direct access is not provided.[80] The present analysis focuses on how the obligation to provide access under Art. 4 affects the scope and practical relevance of the *sui generis* database right. To that end, the following subsection examines with whom the data holder must share data and what conditions apply to such access.

aa) Data shared with the user

Article 4(1) regulates the data holder's obligations vis-à-vis the user. A data holder is defined as a natural or legal person, who has the right or the obligation to use or make data available pursuant to a contractual relationship.[81] In the present scenario, SB Technologies qualifies as the data holder, while FairPlay FC, as the purchaser and user of the smart balls, qualifies as the user.

Where there are several users, the Data Act recognises that each may have contributed differently to the generated data and may independently request access.[82] Since the user bears the risks and enjoys the benefits associated with the use of a connected product or related service, the Regulation provides that the user should also have access to the data generated by the product or service.[83]

Article 4(1) is controversial from both a legal and an economic perspective. In particular, commentators have questioned whether the provision fully realises the objectives of the Data Act, such as facilitating a fair market,[84] given that inferred and derived data are excluded from its scope.[85] Others have argued that Art. 3(2) alone, which is limited to pre-contractual transparency obligations concerning product data and related service data, would not have been sufficient to rebalance data access in practice.[86] Article 4(1) thus represents an important mechanism for enhancing user access to data.

The Data Act is not entirely consistent in its terminology regarding how data are acquired.[87] While connected products are defined as products that «obtain, generate or collect» data,[88] Art. 43 refers only to data that are «obtained from or generated by» such products. Under the definition, a data holder includes data «retrieved or generated» during the provision of a related service.[89] Notably, this wording does not suggest that the data holder must make qualitative or quantitative investments in order to acquire the data, reinforcing the view that Art. 4 targets access to data generated in the ordinary operation of connected products and services.

bb) Requirements for data that are shared

In principle, data are to be directly accessible to users. In situations where this is not possible, the data holder must make «readily available data» and metadata available.

79 G. Lienemann/G.K. Ebner/M. Hennemann/M. Wienroeder, Data Act: An Introduction, Baden-Baden 2024, 82; See also recital 20 Data Act.

80 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 83. For a detailed discussion on the relationship between Arts. 3(1) and 4, see M. Schmidt-Kessel, Heraus- und Weitergave von IoT-Gerätedaten – Analyse des Vertragsnetzes unter dem Data Act, MMR-Beil 2024, 75 ff. Article 4(1) Data Act; In the proposed Data Act, the legal body originally referred to «product» rather than «connected products», despite connected products being mentioned in the recitals. The adopted wording is more precises and better aligned with the Regulation's objectives, cf. recitals 16, 18 and 84 in the proposed Act.

81 Article 2(13) Data Act.

82 Recital 18 Data Act.

83 Recital 18 Data Act.

84 For a general commentary on the debate, see Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 80; for a commentary with a specific focus on Arts. 3 and 4, see W. Kerber, «Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives», GRUR International (2023), who argues that data holders «would get much more from the Data Act than the users with their de facto weak user rights».

85 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 81.

86 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 80 describes Art. 3(2) as an «information-only/transparency-only approach»; See J. Krämer, *Improving the Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act*, Report, CERRE (Centre on Regulation in Europe), November 2022, 10, who argues that «transparency alone cannot be expected to significantly change the competitive dynamics beyond the status quo».

87 See sections III.2 and III.3 above.

88 Article 2(5) Data Act.

89 Article 2(13) Data Act.

«Readily available data» are defined as product and related service data that the data holder obtains or can obtain without disproportionate effort.[90] The Regulation does not specify how «disproportionate effort» is to be assessed, nor what constitutes proportionate effort. Where a data holder refuses to provide access, the burden of proof rests with the data holder to justify this.

In addition to accessibility, the Data Act imposes qualitative requirements on the data that are shared. Data must be made available in a «comprehensive, structured, commonly used and machine-readable format».[91] This wording, which was added in the adopted version of the Regulation, is intended to ensure a certain qualitative standard and to prevent circumvention of the data-sharing obligation. The data holder must prepare the data, together with the relevant metadata, in a manner that allows the user to interpret and to use them.[92] Metadata were not included in the original proposal but were incorporated into the adopted version.

Metadata may take many forms and describe the content or the use of the data produced by the connected product or the analytics platform.[93] Some metadata may be valuable for further development or innovation,[94] and their availability may contribute to breaking down data silos, which is one of the objectives of the circular economy.[95] Since metadata are implicitly included in the definition of a database, obliging SB Technologies to share metadata with FairPlay FC constitutes an interference with the *sui generis* database right.

The data holder may not differentiate between data that are used internally and data made available to the user. Once access is granted, FairPlay FC must receive data of the same quality as those held by SB Technologies.[96] These qualitative criteria are formulated in broad terms, and the Regulation provides limited guidance as to their interpretation. It remains unclear, for example, how discrepancies affect the assessment of accuracy, what degree of completeness is required, or whether the data holder is obliged to verify the reliability of the data prior to sharing. Where verification entails additional costs, the allocation of those costs remains uncertain. These ambiguities are particularly relevant in light of the general requirement that data be made available free of charge.

Further, recital 30 specifies that data made available should be «as accurate, complete, reliable, relevant and up-to-date» as the data accessible by data holder.[97] The Regulation does not require that the data holder already possess such data, but rather that it be capable of obtaining them where necessary. Interestingly, recital 30 refers to data made available to a «third party» rather than explicitly to the user. This has been criticised as a drafting error, with commentators suggesting that the legislature intended to refer to the user.[98] The absence of corresponding quality criteria in the operative provisions of Art. 4(1) further contributes to uncertainty. It would be problematic if such detailed requirements were intended to apply only to third-party access and not to users.

The data holder must make the data available «without undue delay». As this is a concept of EU law, its interpretation should be autonomous and uniform. Guidance may be drawn from the General Data Protection Regulation (GDPR),[99] where «without undue delay» has been interpreted as meaning «as soon as possible» and, where applicable, no later than a month.[100] At the same time, Art. 4 also requires that data be made available continuously and, where technically feasible, in real time. This creates a tension between temporal immediacy and practical feasibility that will need to be resolved in application. It is interesting to consider how «real time» is interpreted in light of undue delay, because if the data are to be shared in real time, it may be too late to grant the user access within one month. It has even been suggested that «undue delay», in the Data Act, may be interpreted as seconds or fractions of a second.[101]

The requirement that data be provided in a machine-readable format is open to interpretation. The Regulation does not prescribe specific technical formats, but merely requires that the data be readable by a machine, which in theory may refer both to autonomously machine-readable files and to OCR-readable files.[102] While this could theoretically

90 Article 2(17) Data Act.
91 Article 4(1) Data Act.
92 This is probably due to that data is «(…) an important input for aftermarket, ancillary and other services», cf. Recital 6 Data Act.
93 Article 2(2) Data Act; Databases consisting of some metadata may also enjoy *sui generis* protection under the Database Directive, see *Innoweb v Wegener* (2013) and *CV-Online v Latvia* (2021).
94 See recital 15 for details on metadata and their value.
95 For further discussion on the role of silos in the circular economy, see B. Sjäfjell/H. Ahlström, Why policy coherence in the European Union matters for global sustainability, Environmental Policy and Governance 2022, 272 ff.
96 There are different opinions on what constitutes quality assessment. For literature supporting the quality criteria in the Data Act, see Max Planck «Position Statement» (2022), 43 note 116. J. Hähnle/K.V. Lewinski (2021), 687 adds «*Nutzbarkeit* (Usability)» and «*Lesbarkeit* (Presentation Quality)» as additional criteria.
97 Recital 30 Data Act. Emphasis added.
98 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 89; «third party» is also mentioned in recital 28 of the proposed Data Act.
99 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 87.
100 See European Data Protection Board (EDPB), *Guidelines 01/2022 on data subject rights – Right of access*, Version 2.1, adopted 28 March 2023, para. 158, interpreting «without undue delay» under the GDPR as meaning «as soon as possible» and, in any event, as within one month. For discussion of how similar timing concepts may operate at the intersection of the GDPR and the Data Act where personal data are concerned, see Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 87; See also S. Richter, Vereinbarkeit des Entwurfs zum Data Act und der DS-GVO, MMR 2023, 166.
101 B. J. Hartman/M. R. McGuire/H. Schulte-Nölke, Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act), Recht Digital 2023, 53: «Sekunden oder in Sekundenbruchteilen»; See also Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 87 for a brief comparison between the Data Act and Article 20(1) GDPR.
102 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 89–90; S. Geiregat, The Data Act: Start of a New Era for Data Ownership? Max Planck Institute for Innovation and Competition 2022, para. 36. OCR-readable files typically refer to scanned physical documents that are rendered machine-readable through optical character recognition, rather than generated natively in digital form.

encompass formats such as PDF or HTML, these formats are unlikely to satisfy the function objectives of the Data Act.[103] The requirements that forms be «commonly used» suggests and emphasis on interoperability and practical useability in the relevant market.[104]

Finally, the requirement that data be made available in a machine-readable and usable format supports the conclusion that pre-processing data in order to render them understandable to the user does not, in itself, amount to an «additional investment» sufficient to classify the data as inferred or derived. Taken together, these requirements significantly constrain the data holder's ability to rely on the *sui generis* right to limit access to data. In the context of professional football, this means that while SB Technologies may retain protection for genuinely derived or inferred datasets, it must provide FairPlay FC with access to raw and pre-processed data, subject to detailed requirements concerning format, quality, and timeliness. Several of these requirements employ terminology familiar from the GDPR, but it is important to note that this article focuses on commercial data. Compared with the legal position prior to the Data Act, this represents an interference with exclusive database rights.

c) Limitations on the data holder's conduct towards the user

In order to ensure the effectiveness of the user's right of access, Art. 4 of the Data Act imposes constraints on the data holder's conduct. These provisions are intended to prevent the data holder from undermining the datasharing obligation through design choices, information requirements, or strategic behaviour.

Article 4(4) provides that the data holder may not make it «unduly difficult» for the user to obtain access to data. The Regulation does not define what constitutes undue difficulty. Commentators therefore refer to the minimisation principle expressed in the recitals to the Data Act, a principle originating in the GDPR and closely linked to the prohibition of dark patterns,[105] which has likewise been incorporated into the recitals.[106]

The minimisation principle implies that the data holder may not request more information from the user than is necessary for the relevant purpose. Dark patterns are choices that are «offered» to the user in a non-neutral manner, or by coercing, deceiving or manipulating the user, or by subverting or impairing the autonomy, decision-making or choices of the user, including through a digital interface.[107] Examples include fake countdowns that require the user to act, or the concealment of necessary information in interface design, so that the user is unable to access it. Where dark patterns are present, the user may disclose more information than is necessary for the purpose of the data collection.

Recital 38 discusses the minimisation principle and differs from Art. 4(4) in two respects. First, Art. 4(4) refers only to the responsibility of the data holder vis-à-vis the user and does not mention «coercing, manipulating or deceiving».[108] Instead, it prohibits impairing the autonomy, decision-making or choices of the user. Recital 38, by contrast, provides that neither the data holder nor third parties may manipulate, mislead or coerce the user, and is therefore more detailed than the provision itself.

A further comparison may be drawn with Art. 6, which regulates obligations where third parties receive data from users. The «unduly difficult» rule also applies to third parties, pursuant to Art. 6(2)(a), meaning that they too must ensure that the process does not become difficult for the data holder and the user. Here, the wording of Recital 38 is repeated, including the references to coercion, manipulation and deception, but the provision applies only in relation to third parties. An open question after studying Arts. 4(4), 6(2)(a) and recital 38 is why coercion, manipulation and deception are not explicitly mentioned in Art. 4(4).[109]

The purpose of Art. 4(5) is to enable the data holder to verify that the user requesting access qualifies under Art. 4(1). Article 4(5) limits the data holder's right to collect information to what is «necessary» for determining whether the requesting party is a natural or legal person, and likewise limits the storage period to what is necessary. The information requested must nevertheless be sufficient to ensure the security and maintenance of the data infrastructure. No requirement is laid down as to how long the data holder must retain the data.[110] This does not mean that the data holder may delete data immediately upon generation. In fact, irrespective of the retention period, the manufacturer must inform the user of the envisaged retention period.[111]

The second sentence of Art. 4(5) reveals the legislator's intention to promote competition. Users are not required to explain why they are requesting access to data, and no examination of clearance by the manufacturer or data holder may be carried out.[112] Accordingly, users need not disclose how the data will be used nor what their business plans

103 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 89.
104 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 89–90, referring *inter alia* to CSV, JSON and XML as «commonly used» formats in several markets. The criteria appear to be inspired by Art. 20(1) GDPR, which requires data portability in a «structured, commonly used and machine-readable format». These conditions have proven difficult to interpret under the GDPR, and similar criticism has been raised in relation to the Data Act.
105 See Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 91. Provisions addressing dark patterns, even where the term is not expressly used, can also be found in Art. 5(1)(a) AI Act, Arts. 5 and 13(6) Digital Markets Act and Art. 25 Digital Services Act.
106 Recital 38 Data Act.
107 Recital 38 Data Act. The wording was first proposed by Council Presidency in 2022; see Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 86.
108 Recital 38 Data Act.
109 Article 6(2)(a) Data Act.
110 By way of analogy, Art. 5(1)(e) GDPR may provide some guidance, although it is neither directly applicable nor sufficient to establish concrete retention obligations in the context of non-personal data addressed in this article.
111 Article 3, recital 24 Data Act; deleting data may violate ‹accessibility-by-design›, Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 91.
112 Recital 21 Data Act.

are.[113] This raises the question of to what extent users can avoid disclosure beyond what is strictly necessary in practice, particularly where connected products require the creation of user accounts before the product can be used.[114]

In practical terms, Art. 4(4) and (5) prevent SB Technologies from requiring FairPlay FC to justify its request for access or from refusing access based on the intended purpose of use. These limitations are likely designed to safeguard the effectiveness of the user's access right and to prevent strategic obstruction, thereby reinforcing the Data Act's competition enhancing objectives.

d) Exceptions to the data-sharing obligation

The previous subsection clarified who may request access to data, and the conditions under which such access must be provided. The present subsection examines the limited grounds on which the data holder, SB Technologies, may lawfully refuse access to data requested by FairPlay FC. These exceptions do not lie at the core of Art. 4 and are therefore addressed briefly. They are, nevertheless, significant as they delineate the outer limits of the data-sharing obligation.

aa) Security

Article 4(2) permits contractual arrangements restricting access to, use of, or further sharing of data where such activities would undermine the safety requirements of the connected product.[115] This is a contract-based prohibition rather than a general prohibition, under which both users and data holders may mutually restrict the access to, use of, or onward sharing of data. This is a strict condition and constitutes a limitation that must follow either from EU law or from national legislation.[116]

To meet the requirement in Art. 4(2), any access, use or further sharing must result in a «serious adverse effect» on the health, safety or security of natural persons. Any restriction must be reported by the data holder to the relevant authorities,[117] who may assist both parties with their expertise. These authorities were not mentioned under Art. 4 in the proposed Data Act, but were added in the adopted version, indicating an intention to adopt a stricter interpretation of the provision, particularly by subjecting security-based refusals to closer scrutiny.[118]

The requirement of a «serious adverse effect» indicates that Art. 4(2) constitutes a narrow exception, which is subject to a high threshold. This interpretation is reinforced by the objectives of the Data Act, which include promoting competition and dismantling data silos. An expansive reading of the security exception would risk undermining those objectives and is therefore not supported by the structure of the Regulation.

bb) Trade secrets

Article 4(6)–(8) likewise set a high threshold. «Trade secret» is defined in accordance with Art. 2(1) of the Trade Secrets Directive,[119] which requires that the information is not generally known or readily accessible, has commercial value because it is secret, and that the entity lawfully in control of the information has taken measures to keep it secret.[120] A trade secret holder is a natural or legal person who lawfully controls the trade secret.[121] In the present example, this would be SB Technologies.

Trade secrets «shall only» be «disclosed» where both the data holder and the user have taken the necessary measures to protect trade secrets. The requirement of necessity is central, yet Art. 4(6) does not specify in which situations such measures may be required.[122] The interest in protecting trade secrets must not be interpreted expansively.[123] Recital 31 explicitly cautions against such an approach, stating that data holders cannot, in principle, refuse access requests solely on the basis that certain data constitute trade secrets, as this would undermine the objectives of the Regulation.

Article 4(7) allows the parties to agree contractually on appropriate protective measures, specifically regarding the measures in Art. 4(6). Where such agreement has been breached, or the parties have not reached an agreement, Art. 4(7) applies and grants the data holder rights to withhold or suspend access to the data. In such cases, the data holder must inform the user in writing if a decision is taken not to grant access. The data holder must also report this to the competent authorities pursuant to Art. 37 of the Data Act. It remains unclear how disputes notified as breaches will be handled in practice, including whether data retention periods continue to run while the competent authority investigates the alleged breach.

Article 4(8) applies only in «exceptional circumstances» where the data holder, acting as a trade secret holder, can demonstrate that disclosure is highly likely to result in serious economic damage. This provision applies only after the measures referred to in Art. 4(6) have been attempted without success. Where the conditions of Art. 4(8) are met, the data holder may refuse access to the relevant trade secrets.

113 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 92.
114 R. Podszun/C. Pfeifer, Datenzugang nach dem EU Data Act: der Entwurf der Europäischen Kommission 2022, 961, arguing that anonymous use of connected devices may in practice be «hardly envisaged at all» («*Die anonyme Nutzung von Geräten scheint gar nicht mehr vorgesehen*»).
115 See Recitals 43, 59 and 61 in the Data Act.
116 Article 4(2) Data Act.
117 Must happen in accordance with Art. 37 Data Act.
118 This addition may reflect an intention to align the Data Act with emerging cybersecurity regulation, as suggested by recital 115 of the Data Act. See, in this regard, Annex I, Art. 13 of the Cyber Resilience Act, which regulates manufacturers' obligations for products with digital elements.
119 Trade Secrets Directive 2016/943.
120 Article 2(18) Data Act, cf. Art. 2(1)(a)-(c) Trade Secrets Directive.
121 Article 2(2) Trade Secrets Directive.
122 The wording concerning «necessary measures» appears to be inspired by Art. 4(3)(c) Trade Secrets Directive.
123 See Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 96, arguing that the mere existence of a trade secret does not, as such, automatically override users' access rights under the Data Act.

The exception in Art. 4(8) is subject to a two-step assessment: first, the likelihood of damage must be high; and second, the anticipated damage must be serious. This cumulative threshold confirms that refusals based on trade secrets are intended to be rare. Allowing refusals too readily would risk neutralising the data-sharing obligation and undermine the objectives of the Data Act. The data holder must further demonstrate the likelihood of serious economic damage on the basis of objective elements.

The literature supports the view that Art. 4(8) will be difficult to invoke in practice.[124] The data holder must demonstrate that such economic damage will occur on the basis of objective elements. It has been suggested that a balancing of the data holder's interests against the user's interests should be undertaken.[125] In order to rely on Art. 4(8), SB Technologies must notify both FairPlay FC and the competent authority in writing. This notification requirement, as with the security exception, reflects the legislature's intention to prevent strategic or unjustified refusals.

Taken together, Art. 4(6)-(8) impose stringent conditions on the invocation of trade secret protection. While these limitations might appear less striking when considered in isolation, they acquire particular significance when viewed in conjunction with the broad data-sharing obligation in Art. 4(1) and the corresponding restriction of the *sui generis* right. In this context, the exceptions confirm that refusals are intended to remain exceptional.

e) Prohibitions imposed on football clubs as users

Article 4(10) and (11) lie at the margins of the analysis but are relevant in illustrating that the user may not use the data for competing purposes or where the data have been obtained through coercion or abuse.

Competing purposes include the development of a competing connected product.[126] This reflects one of the objectives of the Database Directive, namely to prevent parasitic competition. FairPlay FC may not incorporate data from the original product into a competing product, nor share data with third parties for that purpose. Nor may the user derive insights into the economic situation, assets, or production methods of the manufacturer or data holder. In this example the manufacturer and the data holder are the same entity. The limitations in Art. 4(10) do not relate to a geographic market, but to the product market as such.[127]

Article 4(11) further prohibits the use of data where the user discovers vulnerabilities in the technical infrastructure protecting the data. These prohibitions may be characterised as loyalty obligations and are not unreasonable to impose on the user, in our example FairPlay FC.

5. Implications for Smart Ball Providers and Football Clubs

a) Implications under EU law

Article 43 limits the *sui generis* protection for raw data and pre-processed data, while enriched data continue to enjoy *sui generis* protection. SB Technologies is therefore obliged to share raw data and pre-processed data with FairPlay FC pursuant to Art. 4. This obligation is supplemented by qualitative requirements, including that data be shared at the same level of quality as held by the data holder.

Access must be requested by FairPlay FC, placing the extraction and reutilisation conditions in Art. 7 of the Database Directive in an interesting position. While Art. 7 requires the database maker's permission in order to engage in acts covered by the *sui generis* right, Art. 4 of the Data Act imposes a mandatory data-sharing obligation on the data holder, SB Technologies. How this tension will play out in practice depends on how many machine-generated datasets meet the conditions for *sui generis* protection.

Article 4(1) further clarifies that only data obtainable without disproportionate effort must be shared. Thus, SB Technologies is not required to make raw data or pre-processed data available at all costs. Moreover, the interpretation of «real time» as interpreted in case law relating to Art. 7 is interesting due to it being interpreted to constitute extraction. An important difference, however, is that Art. 4(1) regulates data access for a user, i.e. the party directly requesting access, and not for a «data recipient», who would constitute a third party under the terminology of the Data Act.

SB Technologies may refuse access on grounds of security or trade secrecy, but only under strict conditions. SB Technologies may not use «dark patterns» to mislead FairPlay FC, nor may it request information about the purpose for which the football club seeks access to the data. Article 4(10) and (11) impose obligations on FairPlay FC, including prohibitions on competition use and misuse of data. These obligations may be characterised as contractual duties of loyalty rather than manifestations of *sui generis* protection.

b) Comparative note: implications under Swiss law

The following brief reference to Swiss law is included for comparative and contextual purposes only, reflecting the cross-border nature of professional football and data-driven sports technologies.

Swiss law does not recognise a *sui generis* database right comparable to that established under the EU Database Directive. In fact, a legal definition of a database does not even exist.[128] Protection of databases in Switzerland is in-

124 S. Grapentin, Datenzugansansprüche und Geschäftsgeheimnisse der Hersteller im Lichte des Data Act, RDi 2023, 173.
125 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 99.
126 Recital 32 Data Act.
127 Lienemann/Ebner/Hennemann/Wienroeder (n. 79), 99.
128 Instead, the word «*Sammelwerke*» (collections) is used. See Art. 4 Federal Act on Copyright and Related Rights of 9 October 1992.

stead assessed primarily under general copyright law, which requires originality, or under the law of unfair competition. As a result, databases consisting predominantly of machine-generated or sensor-based data, will often fall outside the scope of exclusive protection under Swiss law, unless they meet the higher threshold of creative expression.[129]

Moreover, Swiss law currently does not have a comprehensive framework comparable to the EU Data Act that would impose mandatory data access obligations on manufacturers or data holders of connected products. Under Swiss law, there is no recognition of a *sui generis* right in databases, nor is ownership of non-personal data as such conferred.[130] In general, people who have access to non-personal data are entitled to use them without this amounting to ownership.[131] However, access to certain data may still be restricted by third-party rights.[132] Protection of databases and data-related interests under Swiss law is, instead, achieved through[133] a combination of copyright law, unfair competition law, criminal provisions on trade secrets,[134] and contractual arrangements between the contracting parties.[135]

The limitations on the *sui generis* right under the EU Database Directive and the Data Act apply only within the EU. As the Data Act does not address conflict-of-law issues, questions remain as to the treatment of cross-border disputes. In practice, providers operating in the EU internal market are likely to align their data governance practices with the requirements of the Data Act, even where Swiss law applies only indirectly or contractually.

IV. Conclusion

This article contributes to the existing literature by clarifying how the EU Data Act, through Art. 43, reshapes the practical scope of *sui generis* database protection in data-driven sports contexts, highlighting a shift away from exclusivity. The *sui generis* right has traditionally been interpreted broadly. However, the introduction of a balancing of interests in *Melons* (2021) opened the possibility of weighing database makers' interests against those of competitors and users. This reflects concerns at the EU level regarding the impact of the *sui generis* right on competition and innovation. While the right has been criticised for monopolising information, it has also been defended as a tool for protecting investment, especially by smaller market actors.

The extent to which Art. 43, read in conjunction with Art. 4, limits the *sui generis* protection for databases containing data obtained from or generated by connected products and related services, remains uncertain. This is particularly true for machine-generated data and the boundaries between raw, pre-processed, derived, and inferred datasets. While the Data Act defines data broadly and includes raw and pre-processed data within its scope, it excludes derived and inferred data. Case law suggests machine-generated data may meet Art. 7 of the Database Directive, yet EU policy documents indicate such data should remain outside the scope of protection, highlighting their unclear legal status.

Typical examples of derived and inferred data may include aggregated or model-based outputs, that go beyond the mere recording of events and instead reflect additionally analytical or probabilistic processing. This suggest that the legislature has sought to distinguish between data that are merely generated by connected products and data that result from further aggregation or enrichment, with the latter remaining capable of attracting *sui generis* protection where they reflect substantial investment in the database as such.

The provision imposes a data-sharing obligation on the data holder and at the same time lays down rules on how and when such data must be shared with the user. To prevent the data holder from circumventing this data-sharing obligation, it prohibits so-called «dark patterns» and unnecessary requests for information by the data holder. There are certain exceptions to this data-sharing obligation, justified on grounds of security or trade secrets, but the thresholds are high. The user likewise has a duty of loyalty towards the data holder, which prohibits the user from employing the data for competing purposes and from using data obtained through coercion or misuse.

Taken together, these developments reveal a structural tension between the Database Directive and the Data Act. While the former confers an exclusive right based on substantial investment, the latter significantly limits the practical exercise of that right in contexts involving connected products. Second, legal uncertainty persists as to the conditions under which protection may still be invoked.

To address this tension, greater doctrinal clarity is necessary. In particular, this article argues that *sui generis* database protection should be understood as being exhaustively regulated within the Database Directive itself, and that its scope should not be expanded or effectively redefined through sector-specific instruments where the Data Act already imposes mandatory access obligations. Further clarification would also be desirable in the form of guidance on what constitutes «substantial investment» for the purposes of Art. 7 of the Database Directive, particularly in data-driven environments characterised by automated data generation.[136]

Future research should examine how these dynamics unfold in more complex settings involving multiple investors, as well as situations in which the connected product and the related service are supplied by different entities. Such scenarios are likely to become increasingly common in the sports technology market and will further test the

129 Article 2, Federal Act on Copyright and Related Rights of 9 October 1992.
130 F. Thouvenin/A. Früh, Zuordnung von Sachdaten Eigentum, Besitz und Nutzung bei nicht-personenbezogenen Daten, Zürich 2020, 35.
131 Thouvenin/Früh (n. 130), 9.
132 See Swiss Federal Institute of Intellectual Property, (IGE IPI), Zugang zu Sachdaten in der Privatwirtschaft March 1 2021, 1 ff.
133 As demonstrated in the analysis conducted by Thouvenin/Früh (n. 130), 12–19.
134 See IGE IPI for more details (n. 132), 21.
135 Thouvenin/Früh (n. 130), 32.
136 However, should the *sui generis* right be exhaustively regulated in the Database Directive, such clarification would not be needed.

boundaries of database protection and mandatory data access under EU law.

Zusammenfassung

In diesem Beitrag wird untersucht, wie sich die Datenverordnung (EU-Richtlinie 2023/2854), insbesondere Art. 43, auf den Anwendungsbereich und die Praxisrelevanz des Datenbankrechts sui generis für nicht-personenbezogene, maschinell erzeugte Daten in einem datengesteuerten sportlichen Kontext auswirkt. Anhand eines hypothetischen Szenarios mit intelligenten Fussballtechnologien wird die Wechselwirkung zwischen gesetzlich verpflichtendem obligatorischen Datenzugang und Datenbankschutz analysiert. Dem Unterschied zwischen Rohdaten, vorverarbeiteten, abgeleiteten und gefolgerten Daten wird dabei besondere Beachtung geschenkt. In einem kurzen Vergleich werden die Auswirkungen nach Schweizer Recht erörtert.

Résumé

Le présent article examine l'impact du règlement sur les données (règlement européen 2023/2854), en particulier son art. 43, sur le champ d'application et la pertinence pratique du droit sui generis des bases de données en ce qui concerne les données non personnelles générées par des machines dans le contexte de la gestion de données dans le domaine sportif. À partir d'un scénario hypothétique impliquant des technologies intelligentes dans le domaine du football, le présent article analyse l'interaction entre l'accès obligatoire aux données imposé par le réglement et la protection des bases de données. Il porte une attention particulière à la différence entre les données brutes, les données prétraitées, les données dérivées et les données déduites, et examine les implications en droit suisse dans le cadre d'une brève comparaison.