Opinion of the European Copyright Society on selected aspects of the proposed Data Act

Date: 12 May 2022

Drafting committee: Estelle Derclaye, Mireille van Eechoud, Martin Husovec, Martin Senftleben

Executive summary

The aim of the Data Act's sui generis clause (art. 35) to reduce the availability of IP rights over some datasets is welcome. However, its drafting is flawed and risks creating even more fragmentation in the laws of Member States. To avoid this, article 35 should be amended to make sure that 1) obtaining datasets from usage of Internet of Things products does not qualify as protectable investment under the Database Directive, and 2) the Member States are not allowed to protect the same datasets by any other type of investment protection beyond that envisaged by the Data Act. The revision of the Database Directive that is included in the Data Act does not address the status of public sector data nor does it enable access and use of data for research, but it should.

Introduction: Purpose of the Data Act

The possibility now exists to collect and utilise data generated by the use of products and services in a way that wasn't possible before. But the data is not correspondingly being used and it is concentrated in the hands of relatively few actors. The proposed Data Act (DA) thus proposes to unlock this data and ensure fairness in its access and use.[1] To do so, the DA has five objectives: 1) to facilitate access to and use of data by consumers and businesses including by clarifying the Database Directive 2) to enable the use by public sector bodies of data held by big companies in exceptional cases 3) to facilitate the switching between so-called cloud and edge services 4) to put in place safeguards against unlawful data transfer without notification by cloud service providers and 5) to mandate interoperability standards for data. To these ends, the DA introduces a right of users to access and use the data generated by the use of their products and services, a right to share it with third parties and an obligation for private companies to make data available to public sector bodies to satisfy exceptional needs.

The DA only contains one article relating to the database sui generis right:

> Article 35: Databases containing certain data

[1] Brussels, 23.2.2022, COM(2022) 68 final, 2022/0047(COD), 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).

In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service

1. Relationship between the Data Act and the Database Directive The proposed Data Act is unclear - the database sui generis right can cover observed Internet of Things data

Article 35 assumes that any dataset that falls under the definition of Article 4 DA – "the data generated by its use of a product or related service" – is not protected. Moreover, Article 35 speaks of "*data obtained from* or generated by the use of a product or a related service". Recital 84 explains that "this Regulation should clarify that the sui generis right does not apply to such databases as the requirements for protection would not be fulfilled".

The notion of clarification implies that the investment in the obtaining or generation of such data already does not meet the legal requirements of today's test. However, the statement that such databases would never have been protected under the Database Directive's sui generis right is incorrect.

The sui generis database right undoubtedly can apply to *some* scenarios where Internet of Things (IoT) devices collect data about the use of the products, as defined in Article 2 DA. If the installation of sensors can be viewed as an investment in *obtaining* the data in a given context, it cannot be ruled out that it constitutes a separable relevant investment in the test developed by the Court of Justice of the EU (CJEU) in this respect.[2] Moreover, the definition of the data generated by the use of the "product" is arguably much broader than a typical IoT scenario, such as a smart fridge, or a connected car. In principle, as long as the token used to trigger the transmission of data is physical and communicates through a public communication service, the resulting observed data can qualify (e.g., using a club card in a grocery store).

This means that the DA in Article 35 is trying to achieve a subject matter change — it is trying to change what can be protected.

We do not object to this change. However, if the Regulation really wants to free this type of data from the sui generis database protection, then the currently proposed provision does not achieve that with clarity.

The Data Act wishes to remove legal obstacles that might hinder data access and re-use in the economy. To do so, it wishes to "clarify" what is not protected without at least indirectly amending the Database Directive.

However, any clarification presupposes that the current law does not change. To achieve what the Commission wants, the current law must change. We are of the view that while it is

[2] Case C-444/02, *Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou (OPAP)*; Case C-338/02, *Fixtures Marketing Ltd v AB Svenska Spel*; Case C-46/02, *Fixtures Marketing Ltd v Oy Veikkaus AB;* Case C-203/02, *The British Horseracing Board Ltd v. William Hill Organisation Ltd*.

possible to change the law without re-opening the Database Directive, this necessitates amending it at least indirectly.

In our view, currently protected databases can fall under the definition of datasets of "the data generated by its use of a product or related service" (Article 4 DA). As long as the database maker can prove that such data collection as obtaining of data, and the investment is substantial and separated from the irrelevant investments, the sui generis protection can arise. Thus, for instance, where a person provides gratis a tool to farmers, and that tool collects and sends information to the provider of the tool as it is being used by the farmers, the cost of making and supplying the tools can be regarded as investment in obtaining the data. Therefore, the current version of article 35 of the DA excludes from protection some datasets that would be protected according to the criteria of the sui generis right.

The proposed the Data Act leaves the door wide open for the Member States to enact rights similar to the database sui generis right

Article 35 DA now proclaims that datasets of "the data generated by its use of a product or related service" are *not covered* by the Database Directive. If the courts read this as indirectly amending the scope of the sui generis right, then it effectively excludes such databases from the *scope* of the Database Directive. As a result, there will be no EU law covering such datasets, which in turn means that the Member States are free to legislate there. Article 35 DA does not tell them that they cannot. On the contrary, it confirms that they can legislate in this area.

To avoid this, the Database Directive, including its scope, must be amended at least indirectly, for instance by creating parallel presumptions about availability of the sui generis database protection in the Data Act.

Article 7 of the Database Directive does not cover investment in the *generation* of data (e.g., drawing up flight schedules by airlines). Many IoT databases will be of such kind. The Member States today remain free to design exclusive rights concerning such data *outside* the database sui generis right. Such national rights would not be precluded by the Data Act or the Database Directive. Article 35 DA, as currently drafted helps them to shrug off any concerns about pre-emption by Union law by claiming they are generally outside of its scope.

One could argue that such national experimentation is unlikely. No national parliaments would be interested in introducing such change. However, since the Regulation will *not* require any amendment of the national implementations, it is enough that the courts extend protection on the basis of their existing sui generis right provisions or simply unfair competition laws. The Data Act would not stop this given that such protection would remain outside of its scope. Also, if the Data Act goes far in opening up access to and reuse of data, there is a risk that lobbying at national level will happen to force Member States to do exactly that.

Possible solution

The solution would be to amend Article 35 by including a provision (e.g., as a legal fiction) that data under Article 4 never enjoys, and has never enjoyed protection under the Database Directive. Moreover, to preclude any national experimentation in this space, the clause should also make it clear that the Database Directive extends to such data. One way would be

to extend the scope of the Database Directive to generally cover any investment protection concerning datasets in its definition (Article 4 DA).

In other words, the strategy should be two-fold:

1) To amend the Database Directive by assuring that collection of IoT datasets does not qualify as protectable investment; *and*

2) To prohibit the Member States from protecting these same IoT datasets by any other type of investment protection beyond that envisaged by the Data Act.

In other words, the Data Act should make it clear that databases can neither be protected by the sui generis right, nor can Member States enact national rights similar to the database sui generis right to protect them.

Temporal effects

If there are some databases that fall under the definition of Article 4 that currently enjoy protection, then they need to be stripped of such protection. To make any meaningful difference, such changes should be retrospective, such that the Data Act in that respect also applies to pre-existing databases. Whatever the limitation imposed on the pre-existing rights, we think that other provisions of the Data Act compensate for this loss, by introducing FRAND licensing conditions in case of re-use by third parties.[3] However, as currently drafted, Article 35 does not address these temporal aspects. In our view, given the consequences for these databases makers and possible challenges on the basis of Article 17(2) of the EU Charter, it plainly should.

2. Relationship between the Data Act and the Open Data Directive

The EU has had a long-standing policy to promote the availability of public sector data for re-use. Yet the legal status of data generated by or for public sector bodies for the purposes of exercising public tasks is not harmonized. As a halfway solution, the Open Data Directive[4] prohibits public sector bodies from exercising any sui generis rights where this is unjustified in light of said Directive's obligation to allow re-use. Data held by public sector bodies, but in which third parties own database rights (or other intellectual property rights) are exempted from the Directive. The proposed Data Governance Act[5] seeks to stimulate public sector bodies to also enable re-use of data that is subject to third party intellectual property rights,

[3] See for a similar argument: European Commission, Study to support an impact assessment for the review of the Database Directive. See https://ec.europa.eu/newsroom/dae/redirection/document/83514 p. 58.

[4] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83. Implementation was due July 2021.

[5] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Analysis of the final compromise text in view to agreement, 10.12.2021, Brussels 14606/21 (published on 15.12.2021).

e.g. by clearing rights. However, legal uncertainty as to when data held by public sector bodies is subject to the sui generis right (or database copyright) remains. The proposed Data Act seeks to further stimulate the development and smooth operation of dataspaces and even grants the EC powers and responsibilities to set standards for terms and conditions around data access and use. It does not however consider how a redesign of the sui generis database right could help achieve this. The rationale for having intellectual property rights in databases is primarily that it stimulates the creation of databases and rewards investment risks taken. But for databases produced by or for public sector bodies as part of the exercise of public tasks, this rationale typically does not hold. This is implicitly recognized by the Open Data Directive and the Proposed Data Governance Act, which are aimed at having public sector data 'licensed' as openly as possible, i.e. not hindered by sui generis rights. It would be a missed opportunity if the revision of the Database Directive that is included in the Data Act does not address the status of public sector data.

3. Relationship between the Data Act and the right to research

An effective exclusion of sui generis database protection – following from CJEU jurisprudence and confirmed in Article 35 DA – would eliminate one obstacle to the use of data in the context of scientific research: the use of machine-generated raw data would not amount to an infringement of sui generis database rights – at least as long as Member States refrain from introducing national protection regimes in the absence of harmonised sui generis database protection (see above). This clarification, however, does not automatically offer researchers access to machine-generated raw data. In the absence of sui generis database rights, holders of machine-generated raw data collections may still employ trade secret protection, technological protection measures and contractual obligations to block access to raw data resources.

Therefore, it is of particular importance to clarify whether the proposed Data Act ensures data access for the purposes of scientific research. In this regard, Article 1 DA reveals that the supply of data for scientific research is not the primary purpose of the proposed new legislation. The Data Act seeks to make machine-generated data available to users, trade and business persons and, in cases of exceptional need, to public sector bodies (Articles 1 and 2(7) DA). Given this starting point, researchers can only obtain access by tapping into the data stream to users, or invoking the provisions relating to public bodies.

As to the first option – benefitting from the data stream to users – Article 5(1) DA makes it clear that users may request the sharing of data with a third party "without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time." Recital 29 adds the further clarification that "[a] third party to whom data is made available may be an enterprise, a research organisation or a not-for-profit organisation." EU legislation, thus, explicitly contemplates the possibility of users sharing data with researchers in the context of research projects.

The second option – data access for public bodies – rests on Article 14(1) DA which entitles public sector bodies to request data in situations of exceptional need. Recital 56 points out that "[r]esearch-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law." Hence, researchers in public sector research organisations may be able to rely on Article 14(1) DA and obtain direct

access via this avenue. In addition, Article 21(1) DA allows public bodies that receive data on the basis of Article 14(1) DA to share these data "with individuals or organisations in view of carrying out scientific research or analytics compatible with the purpose for which the data was requested." In cases where a research institution is not organised as a public body itself, indirect data access may thus follow from a collaboration with an eligible public sector body.

Articles 14(1) and 21(1) DA, however, only cover situations of exceptional need, in particular public emergency situations and scenarios where a public sector body depends on the data (which are not available on the market) to fulfil a specific public interest task (Article 15 and recitals 56 and 62 DA). From the outset, the scope of this data access option is thus quite narrow. The use and sharing of data with researchers is only possible under limited conditions. In particular, Article 19(1)(a) DA points out that the data must not be used beyond the purpose which the public body stated in the request for access. Article 19(1)(c) DA imposes an obligation to destroy the data once the emergency situation underlying the research is over. In addition, Article 21(2) sets forth a non-profit requirement. Recital 68 explains this requirement as follows:

> Individuals conducting research or research organisations with whom these data may be shared should act either on a not-for-profit basis or in the context of a public-interest mission recognised by the State. Organisations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Regulation.

For regular scientific research – in the sense of research projects initiated independently by the academic community itself – the public sector avenue (Articles 14(1) and 21(1) DA) has little to offer in the light of the described preconditions for data access. It does not allow researchers to develop the research questions themselves because the research design must be aligned with the exceptional circumstances justifying the data request. Moreover, the emergency situation or other situation of exceptional need can hardly be foreseen. Instead of being self-determined and following an autonomous research agenda, the research reacts to difficult circumstances that have arisen.

In sum, the raw data rules following from the proposed Data Act can hardly be described as a particularly research-friendly regime. Robust access and use guarantees for scientific research are missing. The facilitation of research does not lie at the heart of the proposed new legislation. This is a serious flaw. With the increasing importance of data – and broad access to data – for understanding social, cultural and economic developments, it is indispensable to facilitate research access to data in the framework of the Data Act. In the current draft, the norms that address data use for research purposes only appear as accessory rules that add a research perspective to the primary access provisions for users and public sector bodies without tailoring these rules to the specific needs of researchers and research projects. In the proposed regulatory matrix, the most promising access instrument for research teams is the option of obtaining data as a result of sharing requests which users make in favour of a research organisation as a third party. However, it is an open question whether, in practice, this access avenue – which depends on user collaboration – offers sufficiently broad data access to compile representative data samples that allow scientifically sound analytical work. As for the relationship between the Data Act and the Open Data Directive, it would be a missed opportunity and a severe setback for data-driven research initiatives if the Data Act did not facilitate research.

Signatories

Prof. Valérie Laure Benabou, Professor, Université Paris Saclay / UVSQ, France

Prof. Lionel Bently, Professor of Intellectual Property Law, University of Cambridge, United Kingdom

Prof. Estelle Derclaye, Professor of Intellectual Property Law, University of Nottingham, United Kingdom

Prof. Thomas Dreier, Director, Institute for Information and Economic Law, Karlsruhe Institute of Technology (KIT), Germany

Prof. Séverine Dusollier, Professor, School of Law, Sciences Po, Paris, France

Prof. Christophe Geiger, Professor of Intellectual Property Law, Luiss Guido Carli University, Rome, Italy

Prof. Jonathan Griffiths, Professor of Intellectual Property Law, Queen Mary, University of London, United Kingdom

Prof. Reto Hilty, Director, Max Planck Institute for Innovation and Competition, Munich, Germany

Prof. Martin Husovec, Assistant Professor, London School of Economics and Political Science (LSE), LSE Law School, United Kingdom

Prof. Marie-Christine Janssens, Professor of Intellectual Property Law, Head of CiTiP (Centre for IT & IP Law), University Leuven (KU Leuven), Belgium

Prof. Martin Kretschmer, Professor of Intellectual Property Law, University of Glasgow and Director, CREATe, United Kingdom

Prof. Péter Mezei, Associate Professor, University of Szeged, Hungary; Adjunct professor (dosentti), University of Turku, Finland

Prof. Axel Metzger, Professor of Civil and Intellectual Property Law, Humboldt-Universität, Berlin, Germany

Prof. Alexander Peukert, Goethe-Universität Frankfurt am Main, Germany

Prof. João Pedro Quintais, Assistant Professor, University of Amsterdam, Institute for Information Law (IViR), Netherlands

Prof. Marco Ricolfi, Chair of Intellectual Property, Turin Law School, Italy

Prof. Ole-Andreas Rognstad, Professor of Law, Department of Private Law, University of Oslo, Norway

Prof. Martin Senftleben, Professor of Intellectual Property, Law and Director of the Institute for Information Law (IViR), University of Amsterdam, Netherlands

Prof. Caterina Sganga, Associate Professor of Comparative Private Law, Scuola Superiore Sant'Anna (Pisa), Italy

Prof. Alain Strowel, Professor, Saint-Louis University and UCLouvain, Belgium

Prof. Tatiana Eleni Synodinou, Associate Professor, University of Cyprus, Cyprus

Prof. Mireille van Eechoud, Professor of Information Law, University of Amsterdam, Institute for Information Law (IViR) Netherlands