Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments on

the European Data Act proposal

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Stephan Mietke
Director
Telephone: +49 30 1663-2325
E-mail: stephan.mietke@bdb.de

Berlin, 12 May 2022

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

Preliminary remarks

We welcome the objective pursued by the proposal for a European Data Act, namely to establish a horizontal legal framework to facilitate the access to data for, and the exchange of data between, consumers and businesses. Data-driven innovation and services are becoming increasingly important, both for individual businesses and the European economy as a whole. This requires not only access to data along the entire value chain across the different service providers involved, but also access to data from very different areas of application and industry contexts in order to better understand and meet customer needs.

Customers should therefore be enabled to access the data they provide or generate and to share these data with third parties via a digital interface, preferably in real time, so that the data can be seamlessly integrated into business processes and thus generate immediate customer added value for the company or consumer.

With this in mind, we support the proposed new obligations with respect to accessing the data that customers generate by using connected products and related services. But we believe that limiting the scope to machine-generated data does not go far enough since this will fail to cover a lot of data and thus leave untapped significant potential for new and improved products and services in areas such as banking. This applies, for example, to user data in sectors such as telecommunications, energy and utilities or e-commerce. As we understand it, these data would not fall within the scope unless generated by connected products yet could enable many use cases across sectors and promote greater cross-sectoral reuse of data overall. And last but not least, wider availability of user data beyond the IoT context could make an important contribution to the transition to a green economy.

Supplementary sectoral regulation of individual European data spaces, such as that announced by the European Commission for a separate open finance framework, would run counter to an integrated data economy given the cross-sectoral added value potential of many data and sectoral boundaries which are becoming increasingly blurred. Any sectoral rules should at most support this uniform framework in areas like standardisation but should not create diverging or excessive regulation, not least in the interests of a level playing field.

Against the backdrop of the growing market penetration and diversification of non-European tech giants and platform service providers, we strongly support the exclusion of gatekeeper platforms within the meaning of the Digital Markets Act from the scope of eligible data recipients pursuant to the Data Act. This will help to reduce existing imbalances in the market.

Regrettably, the legislative proposal confines itself to regulating mandatory data access and lacks rules on the voluntary provision and use of data. We believe such rules would be desirable as a basis for facilitating the emergence of European data spaces.

Furthermore, it must be ensured that complying with obligations under the Data Act will not run counter to other statutory or legal requirements or lead to a breach of contractual obligations.

B2C and B2B data sharing (Chapter II)

We support the requirements set out in Articles 3 to 6 of the legislative proposal for new rights to access and share data generated by consumers and businesses with the aim of increasing data sovereignty and making data available for use by third parties.

In their capacity as a third party, banks could then receive and evaluate data generated by the user upon the user's request. This will allow banks to offer their customers new or improved services based on usage data in areas such as lending or payment services. To enable banks to continue in the future to perform this role if their customers so wish, there should be as few restrictions as possible on the ability to receive and evaluate these data.

Although the Data Act is intended to set rules across sectors, it will only affect manufacturers and users of connected physical products (as well as third parties in their capacity as data recipients), which will substantially limit its scope.

It should be borne in mind that competitively sensitive data may also be subject to the right to access and share data. Yet Article 101 of the TFEU prohibits the disclosure of data that allow conclusions to be drawn about certain competitive parameters (e.g. prices, customer-specific information, sales figures, capacities, developments, strategic planning). As a result, data holders and data recipients may find it extremely difficult in practice to determine which data can legally be made available without infringing competition law.

Obligations for data holders (Chapter III)

We welcome the proposed requirement in Article 8 for conditions governing access to data to be agreed between the data holder and the data recipient, including the stipulation that they be fair, reasonable and non-discriminatory. In particular, the ability under Article 9 for the data holder to request reasonable compensation from the data recipient for making data available takes account of the need for a fair balance of interests between the parties involved with the associated costs and benefits in mind.

By contrast, we believe that the proposed ability under Article 9(3) to invoke other Union law to exclude or limit compensation is too far-reaching and incompatible with the Data Act's objective of establishing a consistent horizontal legal framework.

In the area of payment services, data holders currently have no possibility of obtaining adequate compensation when it comes to giving third-party providers access to payment account data. Banks have long been required by the Second Payment Services Directive (PSD2) to make account data available to third-party providers via standardised interfaces whose construction and operation generate substantial costs but for the use of which no fee may be charged. We would welcome it if banks were permitted to obtain compensation for allowing access to data in connection with these services and if PSD2 were amended to correct the imbalances that have arisen in this area. European lawmakers should neither prohibit nor

mandate compensation for data transfers in the banking sector but allow market participants to find appropriate solutions.

We also see a need to spell out to which data provision obligations the rules in Chapter III refer. It is not totally clear whether these rules cover only data sharing between private data holders and data recipients or also data sharing with the public sector. It would be desirable, for example, to have a dispute settlement mechanism for disputes involving the obligations to make data available to public-sector bodies under Chapter V of the proposed Data Act.

Provision of data to the public sector (B2G) (Chapter V)

In principle, we support the objective of enabling the public sector to make decisions based on sound data and to benefit from the increasing availability of data in the digital age. It should nevertheless be borne in mind that the public sector already has extensive data resources at its disposal and priority should first be given to making effective use of these. Additional access to private-sector data should only be considered where there is no alternative, such as in an exceptional emergency situation.

We are concerned that the envisaged requirements in Article 14 et seq. for making data available to the public sector may lead to excessive requests and tie up considerable resources at affected companies, especially since there is no discernible restriction on the obligation to provide data in response to a direct request from any public body. Among other things, we see a need for an ex-ante control mechanism to ensure the proportionality of requests for access to data. If the decision is solely up to the requesting public body, which will have an interest in obtaining the data, the process will lack the necessary impartiality. On top of that, it is totally unclear what criteria will be used to select which companies should provide the data. This opens the door to arbitrary decisions and may disadvantage certain market participants.

Nor is it clear how potential misuse or a breach of sensitive data can be effectively prevented and how those affected can assert claims for damages if necessary. The obligation under Article 19 for public-sector bodies to have measures in place to safeguard the data protection rights of data subjects and protect trade secrets and intellectual property is insufficient, in our estimation, and will undermine the principles of the rule of law. We also have serious reservations about the provision in Article 21 permitting public-sector bodies to pass on data to third parties for scientific research or other analysis without the consent of the data subject. Data holders should have the right to control whether their data are shared with third parties if the data are not anonymised before being shared.

Care should be taken to ensure that the Data Act does not conflict with other EU or national laws or regulatory requirements, such as the GDPR or relevant national regulation, or with contractually binding agreements. It should be clearly defined how the Data Act will interact with other legislation and which law will take precedence.

Furthermore, appropriate data security measures will need to be in place when a business shares data with other organisations. This is not only necessary to comply with regulatory requirements but is also of essential importance to the company itself. Data must be secured by measures commensurate with the need for protection, regardless of who they are shared with.

In addition, there are many areas where public authorities already have extensive rights to access various data in order to perform the tasks entrusted to them. This applies especially to supervisory authorities in the financial sector and the data they require for the purpose of ensuring financial stability. It should be made clear the provisions of the Data Act will not apply to cases where a legal basis for accessing data already exists.

Switching between data processing services (Chapter VI)

The envisaged arrangements for removing obstacles to effective switching between providers of data processing services generally have our support. They will help to reduce market asymmetries and eliminate vendor lock-in by strengthening the rights of customers of data processing services in a highly concentrated market.

It will be essential, however, to avoid excessive intervention in the market. Otherwise, data processing service providers may withdraw from the market altogether or obstacles to market entry by new providers may be created. This could end up reducing supply and thus have the opposite effect to that intended by actually constraining competition.

We do not consider it either desirable or feasible to require complete portability of all the functionalities of data processing services, especially as applications become more complex. Doing so would hamper market innovation and the use of future technologies.

Given the usual complexity of data processing services in the financial industry and in view of the regulatory requirements they have to comply with, we believe that the envisaged maximum period of 30 days for transferring data from one service provider to another is much too short and would be impossible to implement in practice. We therefore recommend permitting longer periods to be contractually agreed.

We see a need to make it clear precisely which data processing service providers would be affected by Articles 23 et seq. Article 2(12) defines the term “data processing service” very broadly. Where Chapter VI aims to facilitate switching mainly between cloud and edge services (see recital 69), clear legal definitions are needed. This is because data processing nowadays forms part – to varying degrees – of many business processes performed by various entities, not necessarily just cloud and edge service providers.

Interoperability (Chapter VIII)

Improving interoperability is an important factor for both individuals and businesses. It will reduce dependence on one provider and make it easier to switch to another provider or implement an exit strategy. Interoperability will enable services to be easily switched between providers without compromising functionality, integrity or availability.

To ensure interoperability, uniform standards for data formats and interfaces need to be developed or defined. We see a need to clarify beyond the provisions of Articles 28 and 29 who will develop these standards and how. In principle, we would recommend a market-driven solution (self-regulation) since this can best meet the needs of stakeholders.

Standardisation processes must nevertheless be transparent and enable the involvement of all relevant interested parties. International standards and standardisation bodies should also be taken into account in the development process. We believe that delegated acts to define framework conditions for interoperability would make good sense. These should be compatible with existing regulatory and supervisory requirements for the financial industry, however.

Article 28 specifies concrete interoperability requirements for operators of data spaces. In the absence of a definition of "data space", however, it is not clear precisely what is meant by the term or who would be considered a data space operator. This needs to be clarified.

We believe that smart contracts have huge potential for agreeing and automating the exchange of goods and services between individual contracting parties both in and beyond the context of the internet of things. Regulating smart contracts exclusively in the context of data sharing, as envisaged in Article 30 of the proposal, does not go far enough. The following example illustrates why: a company finances its connected machinery on a usage basis, i.e. the instalment to be paid to the financing bank is calculated according to the extent to which an individual machine has actually been used. With the help of a smart contract, the usage data could be made available to the bank on a specific date by storing it (encrypted) on the blockchain. However, the use of the machine also gives rise to a claim for payment to the financing bank in the form of a lease or loan instalment, which would ideally be covered by the smart contract as well. In this case, the smart contract would not only govern the shared use of data (as the basis for calculating the loan or lease instalment) but would also trigger an – ideally – fully automated payment by the company to the bank. But existing payments law makes this difficult by assuming that a payment will be manually authorised by the payer and authenticated by the bank, thus generating legal uncertainty and complexity if a payment order is fully automated. These challenges are primarily the result of general civil law principles, which require orders always to be placed by a person.

This example makes it clear that the framework conditions governing smart contracts need to be regulated much more extensively than currently envisaged by the data-related scope of the proposal. Piecemeal regulation in different areas of application risks giving rise to an inconsistent legal framework that will frustrate the commercial spread of smart contracts.

Lawmakers therefore need to take a holistic approach to smart contracts within the meaning of Article 2(16) in the light of other relevant legislative texts and their suitability.

Other comments

In addition, we welcome the measures that Article 27 (Chapter VII) will require providers of data processing services to take to protect data from access by governments in third countries.