Brussels, 12 May 2022
FINAL

EACB Position Paper on a Proposal for a Regulation on "Harmonised rules on fair access to and use of data" (The Data Act)

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.700 locally operating banks and 52,000 outlets, they serve 223 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 87 million members and 705,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the possibility to contribute to the discussion on the Data Act legislative proposal.

General remarks

We appreciate the European Commission's effort to create a more integrated and functional digital single market through the data strategy. We support the Commission's general principle of facilitating the sharing of data. Sharing should be based on free choice, voluntary and on a contractual basis. We believe that the Data Act and the upcoming financial data space should be based on the European principles of a market economy with freedom of contract to allow for sustainable business models to develop and a level playing field for all economic actors with a fair business model for all participants. Contractual frameworks have the benefit of allowing arrangements to be laid down between different parties in a financial transaction chain to manage errors, mistakes, queries, customer complaints and responsibilities.

We believe the following observations are important to keep in mind as background:

- The EACB has looked at the Data Act with particular attention as this additional horizontal proposal sits between the other recent horizontal legislation, i.e., the Data Governance Act, and the upcoming sectoral legislation for the financial sector, i.e., the Open Finance Framework. These are two relevant building blocks for establishing key rules and principles for an open data economy that we strongly believe should be multilateral and cross-sectoral.
  Considering the number of laws, e.g., the General Data Protection Regulation, the e-Privacy Directive, the Second Payment Services Directive, the Data Governance Act, the Digital Markets Act, and the Data Act, consistency among current and new rules is key.

- The EACB shares some of the concerns expressed by the European Data Protection Board (EDPB) in its statement[1] on the Digital Services Package and Data Strategy, especially on the great importance to avoid ambiguities in the Data Act to ensure legal certainty and coherence with the existing data protection framework to ensure its effective application. This first statement has been followed by the recent EDPB and EDPS joint Opinion[2] specifically addressing the Data Act proposal. The Opinion confirms the impression we had while reading the proposal, which is that the boundaries between personal and non-personal data are blurred. We share some of the concerns addressed in the Opinion, such as the interplay between the Data Act and other relevant legislation (as stated in the previous point), the consistency of definitions with the GDPR and the DGA and the obligation for businesses to share data with governments.

[1] EDPB Statement on the Digital Services Package and Data Strategy Adopted on 18 November 2021.
[2] EDPB-EDPS Joint Opinion 2/2022 on the Proposal on harmonised rules on fair access to and use of data (Data Act).

- In the data sharing area in general and in particular in the use of and access to data generated by connected products, a clear distinction between personal data and non-personal data as well between data observed/provided and data inferred/derived is of paramount importance to avoid different interpretations and consequently application and enforcement of the relevant rules. We welcome the specification in Recital 14 which excludes from the scope of the Data Act data derived and inferred (i.e., "*The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation.*").

EACB's specific comments

Please find below the EACB's comments which follow the Data Act structure.

Chapter I – General provisions: Subject matters, scope and definitions

Connected products in scope

We believe that the connected products in scope should be better and more clearly defined.

Recital 15 explicitly provides examples of products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service. Products that generate data as a result of intentional human input to display, record, or transmit content do not fall under the Data Act. The examples of products listed in the recital are personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners.

We understood from the dialogue with the Commission that when checking the scope, this is not about the data that a product generates, but whether that product orchestrates/manages how devices in scope work. We have been reassured that, with regard to the banking and financial sector, payments, credit cards and ATMs are not considered products or related services under the Data Act. However, this is not expressively stated in the proposal. For this reason, we suggest to also extend the list in Recital 15 to the following products: security dongle, debit and credit card (and their digital equivalents such as digital cards on a smartphone or smartwatch), banking apps, PoS terminals, ATMs, and similar devices.

Definitions

- **Art. 2(6) 'data holder'**: As also stressed by the joint EDPB-EDPS Opinion, the definition suggested in the Data Act does not correspond to the definition of the DGA agreed by the European Parliament and the Council of the EU.

- **Recital 14** specifies that "*electronic communications services include land-based telephone networks, television cable networks, satellite-based networks and near-field*

communication networks." According to the definition used in the European Electronic Communication Code (EECC), near-field communication networks are not electronic communications services. We don't understand the reason of broadening the definition of electronic communications services through the Data Act. For this reason, we suggest deleting the wording "*and near-field communication networks"* or in alternative refer to the EECC definition.

- **Definition on 'connected product'**: We believe a more precise definition of 'connected product' would be beneficial to provide legal certainty. The Data Act defines 'product' Art. 2(2) and in this definition, the article paraphrases the connecting element "*and that is able to communicate data via a publicly available electronic communications service*". However, it is unclear what this exactly means. Moreover, the fact that Recital 14 also mentions 'near-field communication networks' among electronic communication services lets us wonder if certain technologies, such as sensors, chips or QR codes are also within the scope. Clarifications in this regard are needed.

- **Art. 2(10) 'public emergency'**: We believe that the definition of public emergency in Art. 2(10) ("'*public emergency' means an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s);"*) and more generally the elements that define the exceptional needs (see Art. 15 and our comments under Chapter V) are too broad. We fear the current definition could lead to widespread expropriation of private data for public use, with little or no compensation for the data holders, and public authorities' use of personal data possibly beyond the scope of and not in line with the GDPR. The latter could possibly lead to an increase of litigation by data subjects towards data holders, given data holders' already existing obligation to comply with the GDPR.

- **Art. 2(17) 'electronic ledger'**: We acknowledge that the suggested definition refers to the definition in the eIDAS Regulation, which is currently under review in the Digital Identity (DI) proposal. The EACB together with the European Banking Federation and the European Savings and Retail Banking Group – jointly known as the European Credit Sector Associations (ECSAs) – are following the DI proposal closely and suggested amending the definition of electronic ledger. The term "ledger" has two meanings: The first is that of Distributed Ledger Technology (DLT); the second meaning is that of bank ledger or ledgers for booking systems in companies (traditional meaning). The EACB, together with the ECSAs, believes that the definition in the DI proposal should be focused on electronic ledgers in the ID context only, otherwise all electronic ledgers (including "normal accounts") would be part of the DI Regulation and would imply double regulation for banks.

Chapter II – B2C/B2B data sharing & Chapter III – Obligations for data holders legally obliged to make data available

The EACB welcomes the inclusion in the Data Act of two important aspects for the relationship between the data holder and the data recipient:

- The prevention for the data holder of any negative impact on its business opportunities. Indeed, Art. 6 set the obligation for the third party receiving the data to not use the data it receives to develop a product that competes with the product from which the accessed data originate.
  Although we do welcome this principle, we would like to also stress that not only should the third party not use the data it receives to develop a competing product but also related services.

- The compensation for the costs of making data available (Art. 9).

However, we would like to stress two key principles here, which are important to always keep in mind, especially in a data economy context: the principle of a level playing field and the principle of proportionality.

1) With regard to the B2C and B2B data sharing, Art. 7.1 exempts micro and small enterprises as defined in Art. 2 of the Annex to Recommendation 2003/361/EC from Chapter II.
   We believe this would constitute an unlevel playing field that could hinder innovation. We believe that the exemption should be more targeted. In order to find a balance between the abovementioned two principles, we suggest limiting the exemption to micro and small enterprises unless such micro and small enterprises provide IoT or data services as core business solutions.

2) With regard to the compensation principle, Art. 9.2 and Art. 9.3 also raise concerns.
   - By limiting the compensation due by micro, small or medium enterprises (SMEs) to the "costs directly related to making the data available to the data recipient and which are attributable to the request", Art. 9.2 would constitute an unlevel playing field. We suggest limiting the exemption to microenterprises only so as to achieve more proportionality in the application. Paragraph 2 read together with Recitals 42 and 46 only refer to cost incurred and investment required for making the data available. However, we believe that there are additional costs that need to be considered, such as maintenance, cybersecurity and overhead costs. Consequently, the compensation should be broadened.
   - With regard to Art. 9.3, the proposal leaves the possibility that other (sectoral) Union law or national legislation implementing Union law could exclude compensation for making data available or provide for lower compensation. This paragraph goes against the level playing field and may lead to market asymmetries and incoherence. We believe that the possibility to exclude compensation for making data available or providing it for lower compensation should only be allowed in exceptional circumstances and would have to be duly justified. Any new EU legislation or review of existing EU legislation should take into consideration the need to achieve a level playing field.

The Data Act deals with a variety of aspects (the B2B and B2G data sharing, unfair terms related to data access, switching between data processing services providers, etc.). Although we believe Chapters I–III regulate the data generated by products (IoT) it is not straightforward to

understand the application of the different Chapters. For example, Chapter III sets out general rules applicable to obligations to make data available where a data holder is obliged to make data available to a data recipient as in Chapter II or in other Union law or Member State legislation. From our exchange with the Commission, we understood that Chapter III is applicable across all sectors in cases where there exists a legal obligation to make data available but not in situations where, for example, financial institutions should provide data/information based on reporting obligations to the authorities. We are reassured about this, and we also noted a very light reference in Recital 59 to this aspect. However, a more explicit and clear reference in the legal text that data provided by financial institutions to Member State and EU competent authorities does not fall under Chapter III would be welcome.

Finally, we believe it would be useful if in Art. 8.1 the date mentioned in Art. 40.1 was repeated or referred to, in order to make clear that Art. 8 only applies to "new" legislation.

Chapter IV – Unfair terms related to data access and use between enterprises (B2B)

We welcome Art. 13 of the proposal as it draws up a list of clauses when a contractual term is unfair and presumed unfair as well as when it should be considered to be unilaterally imposed. However, we believe that all enterprises – no matter the size of the company (big actors could also experience difficulties as micro, small or medium-sized enterprises meet in the contractual negotiation, with even bigger ones) – should benefit from the safeguards set by this article with regard to unfair contractual terms.

Chapter V – Making data available to public sector bodies and union institutions, agencies or bodies based on exceptional need (B2G)

As a general comment there are already laws at national level which define and regulate public sector bodies' access to and re-use of private sector data when such data is needed to carry out their tasks in the public interest. In general, public interest is the subject of extensive legislation at national level.

We understand the importance of enhancing the ability of public authorities to take action for the common good, with the COVID pandemic a real and concrete example. However, we believe that some adjustments to this Chapter are needed:

- **Paragraph 1 of Art. 14 on obligation to make data available based on exceptional need:** As a general consideration, practical experience has shown that companies have always provided support in times of crisis and public emergencies on a voluntary basis. The need to have general obligations in place therefore appears to be disproportionate and not well grounded.
  In addition, paragraph 1 (but also the relevant Recitals on the B2G data sharing) generally refers to data. We understood from our exchange with the Commission that the definition of data used in the Data Act as such is very wide as the Commission wanted to be consistent with the Data Governance Act and the Open Data Directive. Recital 14 states as follows: "*The data represent the digitalisation of user actions and events and should*

accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation." Nevertheless, we believe there should be an indication of what type of data could fall within the request by a public sector body or Union institution, agency or body.
We would also like to have it clearly and explicitly stated in the Data Act that when complying with an exceptional need request, the data holder providing the information is considered not to be in breach of other legislation, such as but not limited to the GDPR.

- **Paragraph 2 of Art. 14**: We question the exemption of micro and small enterprises from the scope as the size of an enterprise should not count when it comes to public interest. With regard to this paragraph, in addition to the principle of a level playing field and the principle of proportionality, a third element needs to be factored in: the situation of exceptional need.

- **Point (a) and point (b) of Art. 15 on exceptional need to use data:** More precision could be given about the distinction between point (a) "*where the data requested is necessary to respond to a public emergency*" and point (b) "w*here the data request is limited in time and scope and necessary […] to assist the recovery from a public emergency*".

- **Point (c) paragraphs (1) and (2) of Art. 15** states that *"where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and (1) the public sector body or Union institution, agency or body has been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; […]*". We are concerned that these provisions will allow authorities excessive margin of manoeuvre to argue they should have access to data, without in practice having any hard obligations to pursue alternative methods or to generate the data themselves.

- **Art. 18 on compliance with requests for data:**

    - From the proposal we understand that whenever a public institution defines what data it needs based on exceptional need or for fulfilling a specific task in the public interest, a body that controls or checks that the public institution's request is reasonable is not foreseen. We believe that Art. 18, which considers the possibility of the data holder to challenge the request by bringing the matter to the national competent authority, and Art. 17, which describes when a request is to be considered valid (the requests for data would need to be proportionate, clearly indicate the purpose to be achieved, and respect the interests of the enterprise making the data available), are not sufficient. We need a standardized process for validating data requests in order to prevent this chapter from opening the gate to arbitrary or random requests. In a situation of public emergency, the validation can

be carried out shortly after the data has been provided. However, we think any request has to be checked by a third party.

- Paragraph 2 of Art. 18: We understand that the 15-day period does not necessarily mean that the data needs to be effectively provided within that period. It is the time foreseen for the data holder to react and either accept the request or reject it/or ask for modification. However, we believe that the time period of 15 working days to modify or decline requests by public bodies in cases of exceptional need will likely be difficult to meet due to possible longer periods needed by companies to identify the need for action (e.g., identification of large amounts of data in terms of anonymisation or pseudonymisation needs might consume a more extended period of time), and perform these actions too. Also, letters (a) and (b) do not foresee for exceptions in cases as described above. We suggest adding a third exception, letter (c) new to be considered for cases where the time period to modify or decline the request is not sufficient to judge whether the data requested is available and can be delivered as required, or as an alternative have it better clarified in the recitals (e.g., in Recital 63).

- **Art. 20 on compensation in cases of exceptional need:**

  - Paragraph 1 states that data made available to respond to a public emergency pursuant to Art. 15, point (a) should be provided free of charge. The paragraph seems to only recognise monetary compensation whereas we believe that non-monetary compensation for making data available to public bodies in public emergency situations should be considered, for example tax incentives.
  - Paragraph 2 states that "*Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c), such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin*." We wonder about the notion of "reasonable margin" as it is not clear who would be in a position to define what a reasonable margin is considering that it could be very different from a public or business point of view.

- **Information security measures are not mentioned in Chapter V**. However, according to common standards or the requirements of the banking authorities, companies – and especially financial institutions, categorise their data in risk levels (e.g., low, medium, high, and very high / confidential. Personal data is always high risk/confidential). Any information security measures are based on these categories and cover integrity, authenticity, availability, and confidentiality. According to these information security standards and regulatory requirements, financial institutions have to ensure that the aforementioned security level will be maintained if they provide data to other companies or organizations. Thus, high-risk data always has to be as secure as the measures this risk level requires, even in emergencies. If this data is disclosed, it can harm companies and/or people. Furthermore, financial institutions will not be compliant with the requirements of their national authority if they cannot ensure the set security measures for their data. We

believe that the fact that public sector bodies and Union institutions, agencies and bodies should "*implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects*" (Art. 19 paragraph 1 point (b)) is not sufficient: clearer and more appropriate safeguards regarding common information security standards are needed.

- **Art. 21 on contribution of research organisations or statistical bodies in the context of exceptional needs**: Article 21 does not foresee the possibility for the data holder to prevent the sharing of its data from the public sector body or a Union institution, agency or body to research organisations or statistical bodies or to ask for certain requirements. We believe that the public institution has to ask the data holder to agree to the sharing of data the public sector body intends to pursue with research organisations. Moreover, since there might be situations where data is high risk and the data holder has to apply strict information security measures, the data holder should be able to ask for an appropriate legal framework to ensure the required level of security or for the data not to be shared with third parties at all. It is true that Art. 21.3 refers back to Art. 19. However, we believe that clearer and more appropriate safeguards in terms of confidentiality, authenticity, integrity and availability are needed (see also our point on information security measures) when the data is forwarded to a third party. This is not only necessary because not securing data is very dangerous for a financial institution, but is also required by national banking regulations. If a financial institution was to provide data merely based on the Data Act, it would not comply with the aforementioned security requirements. The joint EDPB-EDPS Opinion also recalls the need for appropriate safeguards, taking into account the potentially sensitive nature of the data at issue, in accordance with Art. 89 GDPR and Art. 13 EUDPR.

- **Banking secrecy**: Although we fully acknowledge the horizontal level of the Data Act, we would like to have it clarified in the text the interaction between the provision of this Chapter and the duty of banking secrecy. Banking secrecy is a well-established legal concept based on domestic Member State legislation and is a conditional agreement between a bank and its client that all foregoing activities remain secure, confidential, and private. The EACB suggests having banking secrecy protected as well as trade secrets in the Data Act.

Chapter VI – Switching between data processing services

Considering the limited effect of the SWIPO Codes of Conduct on cloud switching, the EACB welcomes the Commission's introduction of minimum regulatory requirements of contractual, commercial and technical nature, imposed to providers of cloud, edge and other data processing services, to enable easier switching between such services.

Nevertheless, we have some remarks to make:

- It is not completely clear from the Data Act if all cloud services are in scope. Furthermore, the term "application" is not defined in the Data Act.

- Connection with the Digital Operational Resilience Act (DORA) and the Digital Markets Act (DMA) (especially related to exit processes) should be considered. Once in force, DORA as a whole will raise the bar on cyber resilience in the finance sector, and banks together with cloud vendors have to take this into account.

- Data Act should be synced with EBA's, EIOPA's and ESMA's cloud outsourcing guidelines. Cloud outsourcing for banks is already under tight scrutiny when it comes to outsourcing outside EU/EEA area. The EBA Guidelines on outsourcing arrangements[3] states that "*competent authorities should ensure that EU/EEA institutions and payment institutions are not operating as an 'empty shell', including situations where institutions use back-to-back transactions or intragroup transactions to transfer part of the market risk and credit risk to a non-EU/EEA entity, and should ensure that they have appropriate governance and risk management arrangements in place to identify and manage their risks*" (paragraph 115, page 54). The EBA Guidelines continue saying that "*Competent authorities should be satisfied that they are able to perform effective supervision, in particular when institutions and payment institutions outsource critical or important functions that are undertaken outside the EU/EEA*" (paragraph 119, page 55). A very similar sentence is also present in the ESMA Guidelines on outsourcing to cloud service providers[4] (paragraph 47, page 38). In the same vein go the EIOPA Guidelines on outsourcing to cloud service providers[5] (paragraph 31, point V). Practically, a high percentage of cloud vendors come from non-EU countries and servers are located outside EEA area.

- We believe that a timeframe of 30 days to complete the switching process is too short and not feasible. We wonder why Art. 24.1(a) sets as maximum mandatory transition period of 30 calendar days. We doubt that this period is sufficient, since based on our members' feedback these complex transitions and migrations can take from 6 up to 18 months. In addition, it is not clear from the proposal when this period starts (always at the customer's request even after terminating the contract?). Moreover, we wonder whether this conflicts with the EBA Guidelines on outsourcing arrangements that state that credit institutions, investment firms, payment institutions and electronic money institutions should determine what they need in an exit strategy situation, including how much time it would take (paragraph 108, page 52). The 30-day maximum transition period clearly limits credit institutions, investment firms, payment institutions and electronic money institutions in their actions.

- It is quite demanding for customers, like banks, to list and remember all of their data and application categories as demanded by Art. 24 paragraph 1 point (b). It is true that banks already have to specify the data that will be processed (GDPR and EBA requirements) and application categories exportable during a switching process (EBA requirements) when they negotiate the contract (as part of the exit plan/transfer services) and banks have to

[3] EBA Guidelines on outsourcing arrangements, February 2019.
[4] ESMA Guidelines on outsourcing to cloud service providers, December 2020.
[5] EIOPA Guidelines on outsourcing to cloud service providers, January 2020.

manage their contracts adequately during the term (EBA requirement) and consequently these specifications should be kept up to date. However, an "exhaustive" specification – as specified in point (b) – is in practice not doable. Circumstances and uses change over time, and even if a bank manages this adequately, keeping an "exhaustive" list of all data and application categories would be too demanding to adhere to.

- We wonder if the exception left to providers of data processing services via the "technically unfeasible" wording (see Art. 24 paragraph 2) will not represent a way to escape the mandatory transition period. We noticed that the burden of proof is on the provider of data processing services, but we think this notion should be further specified in order to avoid any future abuse. In addition, and always related to paragraph 2, we wonder why a notification, in case the mandatory transition is technically unfeasible, should be done by the provider of data processing services after the switching request has been made. Art. 24 aims to specify what the "switch" should look like (obligations of the data processing provider) within a contract, so the provider of data processing services should already know in advance that it cannot meet its contractual obligations with regard to the transition (exit/transfer).

Chapter VII – International contexts non-personal data safeguards

We welcome the Commission's ambition to offer specific safeguards by way of providers of data processing services having to take all reasonable technical, legal and organizational measures to prevent such access that conflicts with competing obligations to protect such data under Union law. The effectiveness of the established process has to be assessed.

Chapter VII relates to non-personal data. Regarding personal data, the realization of the European Union and U.S. new agreement "in principle" on a new framework for cross-border data transfer could represent more legal certainty for all the European actors.

Chapter VIII – Interoperability

The Data Governance Act (see Art. 30(g)) also provides that the European Data Innovation Board (EDIB) will support the Commission to identify the relevant standards and interoperability requirements for cross-sector data sharing. Moreover, Art. 30(h)(ii) proposes guidelines for common European data spaces on, among other points, requirements for ensuring interoperability. At the same time, Chapter VIII of the Data Act set out essential requirements regarding interoperability for operators of data spaces (notably Art. 28).

A clarification on the interaction between the provisions on interoperability under the Data Governance Act and the Data Act is necessary.

Art. 28 refers to "operators of data spaces"; however, the Data Act does not provide a definition of who the "operators" referred to are. Clarification in this regard is needed.

Smart contracts

Given the fact that smart contracts are a rather novel matter and there are no commonly agreed/regulated measurements for the listed standards on essential requirements regarding smart contracts (Art. 30.1), we assume that vendors of smart contracts would have difficulties complying with those standards or performing a conformity assessment based upon those (see Art. 30.2) and be held responsible (Art. 30.3). Therefore, we suggest such clauses only be put in place harmonised standards are in place with regard to the outlined essential requirements.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)