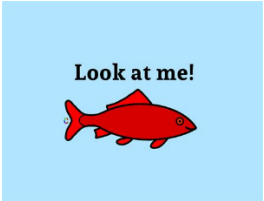
Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford



A red herring

Data protection in light of the EU common data spaces?

A critique of the European Commission Proposal for a Regulation on a Framework for Financial Data Access & of the European Data Protection Supervisor's Opinion on the proposal (Opinion 38/2023), with some broader observations

Conclusion:

The European Data Protection Supervisor's Opinion is a well-meant but ultimately futile and doomed attempt to put parts of a thing – the proposed framework for financial data sharing – into a box – the General Data Protection Regulation – from which it is designed to escape.

In fact, the construct of not-really-consent "permissions" triggering a "legal obligation" to share data, and the attempt to base that data sharing on non-GDPR-based, not Supervisory Authority/European Data Protection Board-approved rules, is nothing more, or less, than a way to get around the GDPR requirements, in particular those relating to consent. It is, in effect, a manifest attempt to undermine the basic principle of informational self-determination.

If the European common data spaces will be created on the basis of this same approach, the GDPR will be completely eroded, and informational self-determination effectively destroyed in whole swathes of socially crucial contexts: health, finance, borders, etc., etc.

The proposal should be rejected as fundamentally undermining EU data protection law in a crucial and sensitive area of consumer activity.

September 2023

Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

Data protection in light of the EU common data spaces?

1. Background:

In 2020, the European Commission announced a "European strategy for data" that would include the creation of a "single European data space", consisting of a series of "common European data spaces":[1]

> The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. …
>
> **The infrastructures should support the creation of European data pools enabling Big Data analytics and machine learning, in a manner compliant with data protection legislation and competition law, allowing the emergence of data-driven ecosystems.**

Two years later, in 2022, it published a Commission staff working document that said that the "key common features" of each common European data space would be:[2]

- A secure and privacy-preserving infrastructure to pool, access, share, process and use data.
- A clear and practical structure for access to and use of data in a fair, transparent, proportionate and/non-discriminatory manner and clear and trustworthy data governance mechanisms.
- **European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected.**

Recently, the Commission issued a proposal for a financial data common space. Below, at 2 and 3, I provide an overview of this proposal, and of the opinion of the European Data Protection Supervisor on the proposal. At 4, I provide my own assessment, in particular as to whether the proposal lives up to the promise that "European data protection [law] are fully protected." I summarise my conclusions at 5.

It should be noted that this is the second proposed common data space. Earlier, in May 2022, the Commission published it proposal for a common health data space.[3] In my conclusions, I add some observations on that proposal, too, and make some broader comments.

---

[1] European Commission Communication on A European Strategy for Data (COM(2020)66final), 19 February 2020, pp. 4 – 5, emphasis added, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066

[2] European Commission, Commission Staff Working Document on Common European Data Spaces (SWD(2022)45final), 23 February 2022, p. 2, emphasis added, available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces
See also the slides for the data.europa academy webinar, Data spaces: Introducing the concept and relevance in today's world, 12 May 2023, available at: https://data.europa.eu/sites/default/files/course/Data%20Spaces_%20Introducing%20the%20concept%20and%20relevance%20in%20todays%20world.pdf

[3] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, (COM(2022)197final), 3 May 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

2. The Proposal

2.1 General

On 28 June this year, the European Commission issued a Proposal for a regulation on a framework for wider access to financial data by certain users, "the FDA Proposal".[4] The FDA proposal was linked to a number of other proposals issued on the same day, including a Proposal for a Regulation on payment services in the internal market, "the PSR Proposal".[5] In particular, the latter regulation, if adopted as proposed, will stipulate that:

> [any] account servicing payment service provider shall provide the payment service user [i.e., the customer][6] with a **dashboard**, integrated into its user interface, to monitor and manage the **permissions** the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments.
>
> (Proposed PSR Regulation, Article 43(1), emphases added; further details are set out in the other paragraphs of this article)

This note is concerned with the data protection implications of the FDA Proposal (hereafter therefore often referred to simply as "the Proposal"), taking the "dashboard" arrangements under the PSR Proposal into account.

As explained in the introductory section to the Proposal, the rationale for the proposed easier and wider data sharing is as follows:[7]

> Customers of the EU financial sector currently cannot efficiently control access and sharing of their data beyond payment accounts. Data users, i.e. firms that want to access customer data to provide innovative services, have problems accessing data held by data holders, i.e. financial institutions that collect, stores [*sic*] and process that customer data. As a result even where customers so wish, they do not have widespread access to data-driven financial services and financial products. A set of inter-related problems explain the limited access to data. First, in the absence of rules and tools to manage data sharing permissions, customers do not trust that potential risks of sharing data are addressed. Therefore, they are often reluctant to share their data. Second, even if they want to share data, the rules governing such sharing are either absent or unclear. As a result, data holders such as credit institutions, insurers and other financial

---

[4] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554 (COM(203)360final) (hereafter: "**the FDA Proposal**" or simply "**the Proposal**"), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0360
The proposal includes the text of the draft regulation.

[5] European Commission, Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (COM(2023)367final) ("**the PSR Proposal**"), available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0367

[6] Note that the term "payment service user" covers both natural and legal persons: see the definition of that term in Article 3(13) of the draft PSR Regulation. See my preliminary comment at 4, below. But this note is primarily concerned with data relating to natural persons and data protection relating to such persons.

[7] Proposal, section 1, Context of the proposal, under the heading "Reasons for and objectives of the proposal", at p. 1.

> institutions holding customer data are not always required to enable the access of data users, like for for example, FinTech companies, i.e. companies using technology to support or provide financial services, or financial institutions that provide financial services and develop financial products on the basis of data sharing to their data. Third, data sharing is made more costly as both the data itself and the technical infrastructure are not standardised and therefore differ significantly.
>
> This Proposal aims to address these problems by enabling consumers and firms to better control access to their financial data.

Following consultations, the Commission concluded that:[8]

> [T]he preferred option is an EU Regulation that establishes a framework for financial data access, which includes the following characteristics:
>
> - require market participants to provide customers with **financial data access permission dashboards** [i.e., those same dashboards as are provided for in the draft PS Regulation] set eligibility rules on access to customer data and empower the European supervisory authorities (ESAs) to issue guidelines to protect consumers against unfair treatment or exclusion risks;
> - mandate access for data users to selected customer data sets across the financial sector, always subject to **permission** by the customers to whom the data relates to;
> - require market participants to develop common standards for customer data and interfaces concerning data that are subject to mandatory access, as part of schemes; and
> - require data holders to put in place APIs against compensation, implementing the common standards for customer data and interfaces developed as part of schemes and require scheme members to agree on contractual liability.

The European Banking Association (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) are to be instructed to issue "**guidelines on the applicable personal data use perimeters**".[9]

While the Commission acknowledges that:[10]

> without appropriate safeguards, more data use could, in specific cases, lead to a risk of higher cost or even further exclusion of customers with an unfavourable risk profile [in particular in relation to] services with inherent risk mutualisation, such as insurance –

---

8 *Idem*, under the heading "*Impact assessment*", at p. 6, emphases added.

9 See Article 7 of the draft regulation. Note that these guidelines will only relate to data sharing "for products and services related to the credit score of the consumer" and "for products and services related to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products" (Article 7(2) and (3)). I return to these guidelines (and certain other rules that are to be adopted) at the end of this section.

10 Proposal, p. 6.

the Commission believes that:[11]

> [t]he Proposal can be expected to have an overall positive social impact provided that the associated risks are kept in check.

It feels that its Proposal achieves this because:[12]

> [s]haring of customer data would be controlled as it is subject to customer request – mandatory access would only be triggered once the customer has requested his or her data to be shared;
>
> data sets which are directly relevant to essential financial services for consumers would be excluded from [the regulation's] scope; and
>
> [the] EBA and EIOPA guidelines on the applicable personal data use perimeters would constitute an additional safeguard.

2.2 Data protection

The Commission claims that the FDA Proposal:[13]

> respects the General Data Protection Regulation (GDPR) which sets the general rules on the processing of personal data related to a data subject and ensures the protection of personal data as well as the free movement of personal data [while at the same constituting] a sectoral building block that fits into the broader European strategy for data and enables data sharing within the financial sector and with other sectors.

The draft regulation does indeed refer in a number instances to the GDPR – *but only in the preambles*. Specifically, while the draft regulation stipulates, in Article 1(4), that:

> [t]his Regulation does not affect the application of other Union legal acts regarding access to and sharing of customer data referred to in paragraph 1, unless specifically provided for in this Regulation –

that paragraph 1 does not mention the GDPR, i.e., it does not contain a provision on the lines of this one in Article 94 of the Payment Services Directive (the directive that the proposed Payment Services Regulation is to replace), referring to the predecessor of the GDPR, the 1995 Data Protection Directive 95/46/EC, and to the data protection instrument then relating to processing of personal data by the EU institutions, Regulation (EC) 45/2001:[14]

> The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.

---

11 *Idem*.

12 *Idem*, but with the sentences broken up and semicolons added.

13 *Idem*, under the heading "*Consistency with other Union policies*", at p. 2.

14 Such "without prejudice to [the relevant EU data protection instruments]" clauses are common in EU instruments that allow processing of personal data. For instance, Article 14(3) of the PNR Directive (also referring to the predecessor of the GDPR, the 1995 Data Protection Directive) stipulates the following:
"This Directive is without prejudice to the applicability of Directive 95/46/EC of the European Parliament and of the Council (13) to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data."

The proposed Payment Services Regulation also does not replicate this provision of its predecessor, stipulating in relation to data protection only that, subject to technical and organisational measures to ensure compliance with some of the principles in the GDPR and in the EU instrument that replaced Regulation (EC) 45/2001, Regulation (EU) 2018/1725, "*payment systems and payment service providers shall be allowed to process special categories of personal data as referred to in Article 9(1) [of the GDPR] and Article 10(1) of Regulation (EU) 2018/1725.*" (Article 80).

Without a clear stipulation in the body of the regulation, on the lines of Article 94 of the PS Directive, quoted above, it would appear that rules set out in the proposed regulation could override the rules in the GDPR, either on the basis that the rules in the proposed regulation are the later ones ("*lex posterior derogat lex anterior*") or because the rules in the proposed regulation are more specific than the ones in the GDPR ("*lex specialis derogat lex generalis*"). That latter view could be said to be supported by the claim made by the Commission that the proposed regulation is "*a sectoral building block that fits into the broader European strategy for data*" (see above).

The references in the preambles do little to fully assuage this concern. Thus, preamble (10) to the proposed FDA Regulation stipulates that:

> [t]he processing of personal data [under the proposed regulation] must **respect the principles of personal data protection**, including lawfulness, fairness and transparency, purpose limitation and data minimisation. (emphasis added)

However, "respecting the **principles** of personal data protection" – i.e., the broad principles set out in Article 5 GDPR – falls far short of having to comply with all the requirements of the GDPR.

Preamble (48) to the proposed FDA Regulation moreover stipulates the following (broken up for easier reading; emphases added):

> **Regulation (EU) 2016/679 [= the GDPR] applies when personal data are processed.** It provides for the rights of a data subject, including the right of access and right to port personal data.
>
> This Regulation is without prejudice to the rights of a data subject provided under Regulation (EU) 2016/679, including the right of access and right to data portability.
>
> **This Regulation creates a legal obligation to share customer personal and non-personal data upon customer's request** and mandates the technical feasibility of access and sharing for all types of data within the scope of this Regulation.
>
> The granting of permission by a customer is without prejudice to the obligations of data users under Article 6 of Regulation (EU) 2016/679.
>
> Personal data that are made available and shared with a data user should only be processed for services provided by a data user where there is **a valid legal basis** under Article 6(1) of Regulation (EU) 2016/679 and, when applicable, where the requirements of Article 9 of that Regulation on the processing of special categories of data are met.

(I will come to the crucial issue highlighted in red below, at 4).

The other references to the GDPR (Regulation (EU) 2016/679) in this preamble relate to a number of more specific issues, i.e.:

> Where the processing of personal data is involved, a data user should have **a valid lawful basis** for processing under Regulation (EU) 2016/679.
>
> The customers data can be processed for **the agreed purposes** in the context of the service provided.
>
> When data processing is necessary for the performance of a contract, a customer should be able to **withdraw permissions** according to the contractual obligations to which the data subject is party.
>
> When personal data processing is based on consent, a data subject has the right to **withdraw his or her consent** at any time, as provided for in Regulation (EU) 2016/679.

However, these preambular considerations – which are not clearly reflected in the legally binding text of the draft regulation itself, which for instance nowhere mentions the term "consent" – do not by themselves ensure that the rules in the GDPR, as interpreted by the Court of Justice, the European Data Protection Board and the European Data Protection Supervisor, will be fully adhered to. How "specific" and "explicit" will the "agreed purposes" have to be? Are all "contractual obligations" limiting the right to withdraw consent – or rather, "permissions": see below – acceptable? Is that a matter to be decided under this instrument (rather than under the GDPR)? It would appear so.

But the most obvious confusion arises in relation to the question of "**permissions**" – a core concept in the draft regulation that is astonishingly not defined in the text of either the proposed PS Regulation or the proposed FDA Regulation. However, the term is (somewhat confusingly) discussed in preamble (69) to the proposed PS Regulation with reference to the Payment Services Directive that that proposed regulation will replace, as follows (references to numbers of instruments replaced with their names):

> The parallel use of the term 'explicit consent' in [the Payment Services Directive] and [the GDPR] has led to **misinterpretations**. The object of the explicit consent under Article 94 (2) of [the Payment Services Directive] is the permission to obtain access to those personal data,[15] to be able to process and store these personal data that are necessary for the purpose of providing the payment service. Therefore, **a clarification should be made to increase legal certainty and have a clear differentiation with data protection rules. Where the term 'explicit consent' was used in [the Payment Services Directive], the term 'permission' should be used in the present Regulation. *When reference is made to 'permission' that reference should be without prejudice to obligations of payment service providers under Article 6 of [the GDPR]. Therefore, permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in [the GDPR]***. (emphases added)

[15] The preamble does not mention it, but "those data" are "personal data necessary for the provision of [payment service providers'] payment services". Article 94(2) PS Directive reads: "*Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the **explicit consent** of the payment service user.*" (emphasis added)

The Commission does not explain what the "misinterpretations" are that it mentions, which leaves its conclusion that "therefore" it should be "clarified" that "*[w]here the term 'explicit consent' was used in [the Payment services Directive], the term 'permission' should be used in the present Regulation*" without clear justification.

It is however very clear that the "permissions" envisaged in the proposed new regulations do not equate to "consent" – let alone "explicit consent" – under the GDPR.[16]

Rather, the very point of using a different term is to have "a clear differentiation" in this respect. Or to put it simply: the financial entities to be covered by the new regulations will not need to obtain GDPR-valid consent for their sharing of (highly sensitive) financial data on customers; some lesser indication of a customer's basic agreement will suffice.

Specifically, as I will discuss further at 4, below, the references in the text of the proposals close to the discussions of or preambles relating to "permissions", to processing on the basis of consent or contracual necessity are basically red herrings in this regard. Rather, once a financial institution obtains this new, lesser kind of "permission", the institution is **legally obliged** to share the data – and consent and contract then become irrelevant. As it is put clearly in preamble (10) to the proposed FDA Regulation:

> The sharing of the customer data in the scope of this Regulation should be based on the **permission** of the customer. The **legal obligation** on data holders to share customer data should be triggered once the customer has **requested** their data to be shared with a data user. **This request can be submitted by a data user acting on behalf of the customer.**

Finally, in this brief overview, I should mention two sets of guidelines and rules relating to the proposed data sharing. First of all, under Article 7 of the proposed FDA Regulation, the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) are instructed to develop **guidelines** on the data use perimeter. And secondly, the data holders and data users must become members of a financial data sharing scheme (FDSS) and adopt rules and standards for those schemes. Preamble (25) to the FDA Proposal says that:

> Financial data sharing schemes must comply with Union rules in the area of consumer protection and data protection, privacy, and competition. The participants in such schemes are also encouraged to draw up **codes of conduct similar to those prepared by controllers and processors under Article 40 of Regulation (EU) 2016/679 [=the GDPR].** (emphasis added)

---

[16] Article 3(11) of the GDPR prvides the following definition:
"*'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*."
Under Article 9(2)(a) GDPR, consent must be "explicit" for the processing of the categories of sensitive listed in Article 9(1), i.e.: "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the … genetic data, biometric data [when used] for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*" The EDPS rightly notes that many of the customer data covered by the proposed FDA Regulation constitute such sensitive data: see EDPS FDA Opinion, para. 13; and financial data is also generally highly senstive, even if not formally included in the list.

A code that is "similar" to one adopted under Article 40 GDPR is of course not the same as a code that is actually adopted under, and in accordance with, the GDPR. I note the point made by the EDPS in that regard below, and return to this issue, too, at 3.

3. EDPS observations and recommendations

On 22 August, the European Data Protection Supervisor – who must be asked for his opinion on such legislative proposals – issued his opinions on the two Proposals.[17] In relation to the proposed PS Regulation, he recommends that the text should be amended to:[18]

- ensur[e] that the dashboard makes reference to the specific designated payment service(s) for which she or he granted her/his permission;
- ensur[e] that access requests remain limited to what is necessary to provide the requested service;
- ensur[e] clarity regarding the legal basis of access requests;
- allow[ ] ASPSPs [account servicing payment service providers] to verify the permission granted by the payment service user or to introduce appropriate alternative safeguards in the PSR Proposal; and
- ensur[e] close cooperation between competent authorities under the Proposal and data protection supervisory authorities to ensure consistency between the application and enforcement of the Proposal and EU data protection law.

In relation to the latter point, "*[t]he EDPS therefore recommends expressly referring to supervisory authorities responsible for monitoring and enforcing data protection law in Article 93(3) of the PSR Proposal.*"

In relation to the FDA Regulation, the EDPS "*welcome[d] that that the Proposal seeks to empower customers - including data subjects - to decide how and by whom their data is used*," but he also had a number of reservations, and made a series of further recommendations. To paraphrase from the Executive Summary to that opinion, he recommends:[19]

- more clearly circumscribing the categories of personal data to be made available under the Proposal, taking into account the risks for individuals whose personal data would be accessed and used, and explicitly excluding data created as a result of profiling from the definition of "customer data";
- requiring data users to clearly outline, for each request, the specific types of customer data they seek access to;

---

17 EDPS, Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access ("**EDPS FDA Opinion**"), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-382023-regulation-framework-financial-data-access_en

EDPS, Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market ("**EDPS PSR Opinion**"), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-392023-regulation-payment-services-internal-market-and-directive-payment-services-and-electronic-money-services-internal-market_en

18 EDPS PSR Opinion, Executive Summary.

19 EDPS FDA Opinion, Executive Summary.

- prohibiting the denial of the financial services to customers who do not install and avail themselves of the permission dashboard or otherwise enable data sharing by data holders with data users under the Proposal; and
- more clearly identifying and strongly enforcing the "data use perimeter".

He feels that the latter in particular "is necessary to delineate appropriate uses of personal data and to protect vulnerable consumers" and, in that regard:[20]

> welcomes that the Proposal provides for the development of guidelines by the European Banking Authority and the European Insurance and Occupational Pensions Authority, in cooperation with the European Data Protection Board (EDPB).

He merely adds that, in his view:[21]

> To ensure that the guidelines are fully aligned with data protection law, the EDPS considers a **formal consultation of the EDPB** to be necessary. The EDPS also recommends extending the scope of the future guidelines to other relevant financial products and services, such as to mortgage credit agreements, payment services, other insurance products, investment products, and pension products. The guidelines should also elaborate, where appropriate, on the limits for combining 'customer data' with other types of personal data, such as personal data obtained from third party sources (e.g., social media networks or data brokers).
>
> The EDPS recommends ensuring close cooperation between competent authorities under the Proposal and data protection supervisory authorities to ensure consistency between the application and enforcement of the Proposal and EU data protection law. Such close cooperation could be fostered by clarifying the circumstances in which competent authorities may consult and exchange information with data protection authorities.

In fact, the EDPS makes some further points, not repeated in the executive summary, some of which should be noted here.

Thus, in relation to the concept of "**permissions**", he notes that:[22]

> Recital 69 of the PSR Proposal specifies that "*(..) permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679*". The EDPS considers that the term 'exclusively' introduces a degree of uncertainty and does not allow to differentiate clearly between 'permission' (referring to the acceptance of the commercial service by the consumer), on the one hand, and 'consent' (under Article 6(1)(a) GDPR) or 'explicit consent' (under Article 9(2)(a) GDPR), on the other hand. Recital (69) should therefore be amended to clarify that "*permission should not be construed as 'consent' or 'explicit consent' or 'necessity for the performance of a contract' as defined in Regulation (EU) 2016/679*".

I will return to this issue below, at 4.

---

20 *Idem*.

21 *Idem*, emphasis added.

22 EDPS PSR Opinion, para. 14.

The EDPS is also concerned that account servicing payment service providers (ASPSPs) cannot verify whether an assertion by a payment initiation service providers (PISPs) or account information service providers (AISPs) that they have obtained a new "permission" from a customer. He fears that this "*may lead ASPSPs to share personal data with third parties that have not secured an appropriate lawful ground under the GDPR (or to share more personal data than intended by the user).*"[23]

More generally, the EDPS recommends:[24]

> that further safeguards and limitations should be included concerning the processing of customer data by data users under Article 6, in order to protect individuals against risks to their fundamental rights to privacy and data protection arising from the increased sharing of sensitive financial data under the scope of the Proposal.

This is reflected in the recommendations set out in the Executive Summary, paraphrased above.

Those recommendations appear to try and bring the proposed FDA Regulation requirements more closely in line with the requirements of the GDPR in terms of data necessity and minimisation, purpose-specification and informing of data subjects, etc. But the EDPS does not suggest (as I will do below, at 4) simply bringing the whole data sharing arrangements within the GDPR – including its requirements as to what constitutes valid consent.

Similarly, as noted above, in relation to the proposed guidelines to be issued by the EBA and EIOPA, the EDPS recommends that the EDPB should be formally consulted on the drafts, with the EDPB then issuing an opinion on them.[25]

On the other hand, the EDPS recommends replacing the proposed FDSS codes "similar to those prepared by controllers and processors under Article 40 of [the GDPR" with codes that are actually formally codes under that article.[26]

4. My assessment

As a preliminary point, I am unclear about the implication of the assertion in the FDA Proposal that not all "customer data" are "personal data" within the meaning of the GDPR. As it is put in the very definition of "customer data" in Article 3(3) of the draft FDA Regulation:

> 'customer data' means personal and non-personal data that is collected, stored and otherwise processed by a financial institution as part of their normal course of business with customers which covers both data provided by a customer and data generated as a result of customer interaction with the financial institution.

"Customers" are any "natural or … legal person who makes use of financial products and services" (Article 3(1))

The categories of customer data covered are listed in Article 2(1); they are extensive and include data on mortgages, savings and investments, pension rights, non-life insurance products, and data on creditworthiness assessments.

---

23 *Idem*, para. 17, original italics.
24 *Idem*, para. 20.
25 EDPS, FDA Opinion, para. 30, reflected in recommendation 10, on p. 20.
26 *Idem*, para. 47, reflected in recommendation 22, on p. 21.

To the extent that any such data "relate" to a natural person (even if only by means of a reference or account number), they of course are all "personal data" within the meaning of the GDPR (see Article 3(1) GDPR). To the extent that such data relate to legal persons, they are not "personal data" within the meaning of the GDPR, and perhaps it would have made sense to create a separate instrument on the sharing of legal persons financial data; after all, legal persons (companies, etc.) do not need the same level of data protection as natural persons. But I wonder if the lumping together of these terms is not intended to suggest that "data [on a natural person] generated as a result of customer interaction with the financial institution" may not always constitute "personal data" within the meaning of the GDPR. If this were to be intended to refer to completely anonymised statistical data, that would be correct, but not otherwise. Suffice it to note here that as long as any "generated data" are still linked or linkable to a natural person, they will still be "personal data" and must therefore be processed in full compliance with the GDPR. But beyond that I will leave the issue aside.

Much more importantly, as noted at 2, above, the FDA Proposal in various places, including in recitals, refers to processing of customer financial data on the bases of consent and contractual necessity, i.e.:

> The dashboard will strengthen customer control, notably when personal data is processed for the requested service, based on **consent** or **necessary for the performance of a contract**.[27]
>
> Where the processing of personal data is involved, a data user should have a valid lawful basis for processing under [the GDPR]. … When data processing is **necessary for the performance of a contract**, a customer should be able to withdraw permissions according to the contractual obligations to which the data subject is party. When personal data processing is based on **consent**, a data subject has the right to withdraw his or her consent at any time, as provided for in [the GDPR].[28]
>
> The permission dashboard should display the permissions given by a customer, including when personal data are shared based on **consent** or are **necessary for the performance of a contract**.[29]
>
> (Emphases added)

In fact, all those references are nothing more than red herrings: contrary to what they suggest, the widespread access to and sharing of customer financial data under the proposed FDA Regulation is <u>not</u> based on either of these legal basis, as laid down in Article 6(1)(a) and (b) GDPR:

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given **consent*** to the processing of his or her personal data for one or more specific purposes;
>
> [*NB: This consent must be "explicit" if it relates to sensitive data, as customer financial data often will do: Article 9(1)(a) GDPR]

---

27 FDA Proposal, <u>Explanatory Memorandum</u>, under the heading "*Fundamental rights*", on p. 8.

28 Draft FDA Regulation, preamble (10).

29 *Idem*, preamble (22).

(b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Rather, as is made clear in preambles (10) and (48), already quoted:

> **This Regulation creates a legal obligation to share customer personal and non-personal data upon customer's request …**
>
> **The legal obligation on data holders to share customer data should be triggered once the customer has requested their data to be shared with a data user.**

In other words, the sharing of customer financial data under the proposed regulation would be based on Article 6(1)(c) GDPR, i.e., that:

(c) [the] processing [here: the sharing of customer financial data] is necessary for compliance with a **legal obligation** to which the controller is subject.

The references to consent and contractual necessity are therefore misleading to say the least – in my opinion, they are deliberately deceptive.

The question remains: why? Why put forward a proposal that makes the wider and easier sharing of customer financial data mandatory, a "legal obligation", while pretending that it will "strengthen customer control"? "Customer control", or to use the phrase underpinning data protection, "informational self-determination", rests on consent.

So why is it not simply proposed to facilitate wider and easier sharing of customer financial data with the consent of those customers?

The answer is, apparently, that the use of the GDPR term "explicit consent" in the Payment Services Directive "has led to misinterpretations".[30] As noted at 2, above, the Commission does not clarify what those "misinterpretations" are, but presumably the Commission means that some people understandably took that term in the PSD to mean the same thing as in the GDPR – and the Commission feels that was wrong. So they have come up with "permissions" that do not quite amount to GDPR-valid consent. But of course, in EU data protection terms such not-really-consent "permissions" cannot be a legal basis for the processing.

They therefore performed a neat legal trick: they used the not-really-consent "permissions" as a "trigger" for the application of a (newly constructed) "legal obligation" – and then the legal basis became that legal obligation, and not the not-really-consent "permissions".

In other words: the construct of not-really-consent "permissions" triggering a "legal obligation" to share data is nothing more, or less, than a way to get around the proper GDPR consent requirements.

But of course you do not "strengthen customer control" by undermining the legal basis of consent and replacing it with a legal obligation triggered by something less than consent.

In my opinion, the "permissions trigger a legal obligation" construct is quite simply a fraud, a manifest attempt to undermine the basic principle of informational self-determination.

[30] See the quote from preamble (69) to the proposed PS Regulation on p. 5, above.

In this light, it is surprising that the EDPS was taken in by this, and "welcomed" the proposal in principle.

Rather, the EDPS should have asked why a separate legal instrument on the sharing of customer financial data (where the customer is a natural person) is needed at all.

In my opinion, the proposed FDA Regulation is not needed at all. There is no reason why wider sharing of natural person financial data cannot simply be based on GDPR-compliant freely given, specific, informed and explicit consent., with clarification on relevant matters – what information should be given to the customer, and how and when; how the customer can express this GDPR-compliant consent; etc., etc. – addressed in a code of conduct adopted under Article 40 GDPR, i.e., with a draft code submitted to the competent supervisory authority and (since we are talking about pan-EU activities) the European Data Protection Board for approval.

It is typical for the cynical attempt by the Commission to try and bypass the consent requirements of the GDPR, that the Commission also tries to get away with basing the sharing of customer financial data on non-GDPR-based, not supervisory authority/EDPB-approved guidelines and non-GDPR-based, not supervisory authority/EDPB-approved codes of conduct that is only "similar" to a proper GDPR-based (SA/EDPB-approved) code of conduct.

5. Conclusion

The EDPS Opinion is a well-meant but ultimately futile and doomed attempt to put parts of a thing – the proposed framework for financial data sharing – into a box – the GDPR – from which it is designed to escape.

In fact, the construct of not-really-consent "permissions" triggering a "legal obligation" to share data, and the attempt to base that data sharing on non-GDPR-based, not SA/EDPB-approved rules, is nothing more, or less, than a way to get around the GDPR requirements, in particular those relating to consent. It is, in effect, a manifest attempt to undermine the basic principle of informational self-determination.

The proposal has wider implications for the creation of the European common data spaces mentioned at 1, above. If the approach taken in relation to financial data is also adopted in relation to the other 10 or so common data spaces under consideration,[31] the effect will be to create what will effectively be data protection-light spaces for the enormous amounts of personal data that would be released into these spaces. Those data would be widely shared under rules that are not guaranteed for comply with the GDPR, and that deliberately undermine the power of European citizens to control their personal data.

Some references in the proposal for a European Health Data Space worryingly point precisely in that direction. Thus, it says that, if that space is adopted as proposed:[32]

---

[31] Apart from in relation to finance, common european data spaces are envisaged for health, industrial & manufacturing, agriculture, mobility, energy, public administration, skills, EOSC, and in relation to the European Green Deal. See the Commission Communication on A European Strategy for Data (footnote 1, above), pp. 22 – 23, and the 9th slide used in the webinar referenced in footnote 2, above.

[32] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (footnote 3, above), p. 15.

> **On secondary use of electronic health data, researchers, innovators, policy makers and regulators would be able to have access to quality data for their work** in a secure way, with a trusted governance and **at lower costs than relying on consent.**

That rather gives the game away: "relying on consent" would cost money, and the rules must therefore be bent to facilitate access to highly sensitive data.

If the European common data spaces will be created on the basis of this approach, the GDPR will be completely eroded, and informational self-determination effectively destroyed in whole swathes of socially crucial contexts: health, finance, borders, etc., etc.

- o – O – o –

Douwe Korff (Prof.
Cambridge (UK), September 2023