AK EUROPA

Position Paper
December 2023
Consumers

Financial Data Access

COM(2023) 360

Executive Summary

Background

Similar to the Commission's previously published proposals on the EU Health Data Space and the Data Act, the proposal is aimed at the access to, sharing and use of personal financial data by different data users. The declared aim is to generate "added value" in the form of innovations in the EU-wide financial services sector.

Summarised assessment

- A better balance between the interests of the data economy and those of consumers is needed. Among other things, AK is calling for a separate legislative act that sets precise limits for companies in general and credit agencies in particular for the use of financial and behavioural data for the purposes of assessing and forecasting creditworthiness.
- It should be clarified that insurance products with a health connection and data on the creditworthiness of consumers are not covered by the scope of the draft. Although Art. 2 states this unequivocally, Art. 7 nevertheless creates guideline competences for the EU Commission for the excluded areas.
- The reproduction of fragmentary excerpts from the GDPR should be avoided. This does not create any added value, but unnecessary legal uncertainty regarding the responsibilities of the data protection or financial supervisory authorities.
- It would be desirable to have precise sector-specific requirements that go beyond the general principles of the GDPR, for example with regard to information and consent rights, purpose limitation, data security and advertising prohibitions.
- The undefined term "permission" pervades the entire draft. It should be replaced by the clearly defined term "consent" with reference to the GDPR.
- "Financial data sharing schemes" should be required to store personal data on servers and clouds located within the EU.
- When determining the competent authorities, it should be explicitly stated that the data protection authorities must implement all aspects of data protection resulting from the Regulation.
- The disclosure of traffic data of telecommunications operators should be cancelled without replacement due to a lack of conformity with the case law of the European Court of Justice.

AK's position

General information

The ambitions of the proposal are inevitably in tension with the fundamental rights to data protection and privacy, which take precedence over purely economic interests.

The promotion of competition and new financial service products can certainly be recognised as a legitimate interest. However, both do not generally constitute an overriding legitimate interest within the meaning of the GDPR, behind which the confidentiality interests of consumers would have to take a back seat in a generalised and undifferentiated manner. Consumers must be free to decide whether there should be offers tailored to their personal profile, for example, for which they provide their financial and behavioural data to third parties. The digital self-determination of consumers is the highest maxim: whether, which and for what specific purpose financial data may be shared with each other are decisions that are exclusively reserved for consumers. Even if the draft - as far as can be seen - is consistently based on the consumer's consent requirement for data use, it must be clarified whether consumers can sufficiently understand the scope of their decision and the individual data flows in a technically highly complex market situation.

The draft should therefore also be judged on whether it complies with the fundamental principles of the GDPR: For example, the principle of data minimisation, meaningful prior information on data use, on the basis of which consumers can make an informed and free decision - i.e. without disadvantage - as to whether they consent or not. Opinion 38/2023 of the EU Data Protection Supervisor (EDPS) of 22 August 2023 rightly draws attention to the considerable imbalance of power between consumers and financial institutions. Anyone who needs a loan quickly or is dependent on certain insurance in everyday life is in any case the much weaker party to the contract. As a result, there are often doubts about the voluntary nature and therefore the effectiveness of the declaration of intent. It is an obvious shortcoming of the draft that it does not contain any criteria that concretise the GDPR and can be used to determine whether consent to a data-driven project can be valid at all.

Moreover, in his opinion (p. 10, "The role of permissions"), the EDPS criticises the fact that the term "permissions of the customer" unnecessarily introduces a new term that is obviously different from "consent" under data protection law (GDPR). The intention behind this is unclear and certainly requires clarification.

Basic considerations

AK takes a very critical view of the proposal for several reasons:

- The need for action proclaimed by the Commission because customers are hindered in accessing their data is incomprehensible. AK's consumer counselling service has not yet registered any complaints about a lack of access to data. This data is mostly contract data and contractual information to which customers have access, whether online or in paper form.

- Financial services are very complex products and an extremely sensitive area. On the one hand, because they regularly involve contracts with very large sums of money that consumers only take out once in their lives (mortgage loans or pension provision) or that are associated with a risk of loss, such as many investment products. On the other hand, it is about lifelong contracts such as private health insurance or contracts that serve to cover existential risks (homeowner's, liability and accident insurance).

- Commissions still play a significant role in the sale of financial services across Europe. Negative incentives and their effects have been documented by the BEUC, among others. The legislative proposals on the retail investor strategy do not significantly change these distribution structures. It is to be feared that the proposed wide-ranging access to financial data will

significantly increase the risk of aggressive sales practices, such as the "twisting" of insurance investment products, which is often lamented even by the insurance industry.

- In the digital age, permanent vulnerability must be assumed. The assumption that consumers act confidently when they have access to detailed information is outdated. The trust of each individual can easily be exploited in the digital economy. Manipulation, abuse and "social engineering", for example in the area of online payments, have led to a sharp increase in damage in recent years, which ultimately had to be borne by customers. The Commission's draft is characterised by the model of informed, sensible and diligent consumers, although a departure from this model is necessary, especially in legislation. Instead, we must assume that consumers will be permanently vulnerable in the future.

The main provisions of the draft: The Area of Application

The list includes an enormous range of customer data, such as mortgage credit agreements, loans and accounts (with the exception of payment accounts within the meaning of the Payment Services Directive), including (savings) balances, conditions and transactions, (insurance-based) investment products, crypto assets and real estate. In addition, the credit assessment of companies in the event of a credit application.

Credit reports: The fact that credit assessments of consumers are not covered is expressly welcomed. At the same time, however, AK points out that there is an urgent need for EU-wide standardised data protection regulation of the business of credit agencies and the credit ratings they produce (with or without AI systems). It should be noted that the GDPR has not come close to standardising their business practices (in terms of data sources, data scope, prior information of data subjects, use of and information on automated individual decisions, checking the authorisation of data recipients to query data, storage duration and handling of rectification claims). Unlawful use of data (e.g. data obtained from direct advertising companies or social media), poor data quality, unscientific and therefore discriminatory scoring methods violate the fundamental rights of many consumers and often exclude them completely unjustifiably from participating in business life due to poor ratings.

Health-related insurance products: We agree with the position of the EDPS: It is to be welcomed that life and health insurance policies are excluded from the scope of application due to the high sensitivity of the data involved.

AK concern: The present draft is not directly suitable for the inclusion of consumer-friendly legal requirements for credit ratings. However, AK considers a separate sector-specific directive for the regulation of credit ratings and AI-based scoring of consumer behaviour to be overdue. Not least because the planned financial data space will make much more behavioural data available, which would be particularly attractive for creditworthiness analyses. Appropriate limits must therefore be set on the usability of the data collected by the draft for credit ratings and forecasts. This is the only way to strike a fair balance between the promotion of the data economy through access to personal financial data and the need to protect consumers from unfavourable assessments.

Obligation of data holders to provide customer data to data users

At the customer's request, the data holder shall provide data to data users for the purposes for which the customer has given their permission. Before doing so, the data holder must ask the data user to prove that it has received the customer's authorisation to access the customer data stored by the data holder. In addition, a dashboard for monitoring and managing authorisations must be made available to the customer.

The term "permission" is not defined in more detail and also differs in meaning from "consent", which is a legal basis for data processing under the GDPR.

AK concern: These conceptual deviations lead to unnecessary legal uncertainty and also have no benefit whatsoever. Data holders and data users are and remain controllers within the meaning of the GDPR and are in any case liable for unlawful data transfers and processing that are not covered by valid consumer consent. Legal bases under data protection law other than consent should also not come into consideration, as the draft grants consumers a right of withdrawal without exception, which the GDPR only provides for in connection with the legal basis of "consent". In the view of AK, the data user should therefore have to obtain consent from the consumer that is effective under data protection law. The data holder should have to request the signed declaration of consent and check its effectiveness and scope before passing on the data. If it is worded imprecisely, the data holder must ask the data user to rectify this.

In addition, the data holder should check whether the data user is authorised to exercise the rights as defined in Art. 6 (1).

Obligations of a data user who receives customer data

According to Art. 6 (2), the data user may only access customer data for the purposes and under the conditions for which the customer has given their consent. They must delete them when they are no longer required. The added value of this provision, which arises directly from the GDPR anyway, is not apparent. If the redundant inclusion of the data protection obligations under the GDPR in the current draft is intended to provide for the supervisory authorities for the financial sector as data protection review bodies in addition to the data protection authorities, then it would be more appropriate to address this in the supervisory responsibilities (and to precisely define the exact areas of responsibility and obligations for cooperation between the authorities).

In Art. 6 (4), the data user is (redundantly) obliged once again " to not process any customer data for purposes other than for performing the service explicitly requested by the customer", on the grounds of "to ensure the effective management of customer data". This justification is incomprehensible; "to ensure the effective management of data" is an empty phrase. It fails to emphasise the responsibility of the data user to (naturally) respect the fundamental rights (of customers of a third party).

We also miss the legal quality of the wording of points c) and d). Accordingly, "adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal customer data" shall be put in place and "necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal customer data" shall be taken. It is not clear why the protection of non-personal data takes centre stage in both cases, although the draft consistently addresses personal data due to the type of data (customer data) and the legal basis (consent requirement under the GDPR). It also remains unclear why data security measures are not also required for personal data.

Not much more than - one might almost say - pseudo-protection can be expected from the requirement for data users in point e). According to this, customer data may not be processed for advertising purposes, "except for direct marketing in accordance with Union and national law". It goes without saying that direct marketing is only permitted within the framework of national and European laws. What other conceivable forms of advertising beyond direct marketing are to be excluded remains unclear. Finally, it should be noted that there is no standardised definition of direct marketing in EU legislation (only advertising for the data user's own products or also those of third parties; in the case of third parties, the legal question of EC 47 of the GDPR, which has not yet been clarified by the ECJ, arises: According to this, direct advertising can constitute a legitimate interest, although it is unclear whether this only concerns the data controller's own customers who are advertised with its own products or also direct advertising by third parties who have no contractual relationship with the consumer).

AK concern: The reproduction of short, incomplete excerpts from the GDPR in the current draft does not bring any added value to the affected consumers. However, it leads to considerable and undesirable legal uncertainty as to which authority (data protection or financial supervisory authorities) is responsible for enforcing these obligations. In the interest of consumer protection, AK expects more precise, sector-specific requirements for obtaining consent, limiting the purposes of use, data security and the ban on advertising that go beyond the general GDPR principles.

Scope of data utilisation

The draft recalls that the processing of customer data must be limited to what is necessary for the purposes for which it is processed. This reference is in line with the principle of data minimisation under the GDPR, without going beyond it and making it more precise. As already criticised in Art. 6, a standard without added value is being created here, which leads to legal uncertainty. Both positive and negative conflicts of jurisdiction are to be expected (two or no competent authorities; data protection vs. financial supervisory authorities).

Against this background, AK also firmly rejects the authorisation of the European Banking Authority (EBA) to "develop guidelines on the implementation of paragraph 1 of this Article for products and services related to the credit score of the consumer" or the insurance supervisory authority (EIOPA) in cases "related to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products". Firstly, supervisory authorities for individual economic sectors acquire competences that lie within the remit of independent data protection authorities. The proposed involvement of the Data Protection Committee does not adequately compensate for this shift in competences. Both authorities focus exclusively on the needs of economic operators, but not on the data protection and privacy rights of

consumers. It is therefore only conceivable for the Data Protection Committee to take the lead and issue guidelines in cooperation with the EBA and EIOPA.

Secondly, the question arises as to why a general reference is made to paragraph 1, which in turn refers to Art.2 (1), if the guidelines are only intended to define the appropriate scope of data for very specific areas (consumer creditworthiness and risk assessment for life and health insurance) which are not covered by Art.2 (1). In other words, the crucial question arises as to why guidelines are allowed at all for data categories that do not fall within the scope of the Regulation: According to Art 2 (1) (f), only creditworthiness checks of companies are covered, but not those of consumers. According to Art.2 (1) (e), insurance is generally covered - with the exception of life, health and comparable health-related insurance.

AK concern: The tasks of data protection authorities overlap with those of financial supervision even more clearly than in Art. 6 when principles from the GDPR are reproduced in fragments and without any added value for consumers. The EBA is to be given explicit guideline competence for a task that falls within the core area of the GDPR and thus of the enforcing EU Data Protection Committee (data minimisation, limits of data required for various purposes). AK firmly rejects such an overstepping of competences. It would be conceivable to entrust the EU Data Protection Committee with guideline competences, whereby EBA or EIOPA would have to be involved in the performance of this task. In this specific case, the guidelines should (of course) only cover data categories that fall within the scope of the draft. Consumer credit scores, risk assessment and the setting of premiums for life and health insurance policies are certainly not included, which is why these parts of the standard would have to be omitted without replacement.

Dashboards with access rights to financial data

The data holder should provide customers with a dashboard to monitor and manage the permissions granted to data users. We would like to point out once again that the term "permission" does not necessarily have the same meaning as consent under data protection law. It must be made clear what the differences are, otherwise consumer rights cannot be exercised with legal certainty in practice. The period of validity of the access permission must be indicated on the dashboard (Art.8 (2) (v)). However, the period of access permission is not necessarily the same as for the permitted storage period of the data. Privacy-by-design settings are also necessary for this in order to allow consumers to make a self-determined choice.

AK concern: Since - as far as can be seen - the draft is exclusively concerned with the sharing of personal data, the term "permission" should be replaced by "consent" with reference to the GDPR. Data holders and data users should actually also be treated and referred to as data controllers and recipients within the meaning of the GDPR, as they are in any case addressees of the GDPR and must fulfil their obligations in this regard (if aggregated, "other" data without personal reference is also involved in passing, it would be sufficient to only refer to data holders and data users at these points). Irrespective of the possibility for consumers to exercise their right of cancellation at any time, the maximum storage period for each data category should be indicated on the dashboard. Consumers should be given the opportunity to decide whether they want their data to be physically deleted after the purpose has been fulfilled or whether they consent to further processing for secondary uses beyond the original purpose (e.g. for statistical purposes).

Financial data sharing schemes

The IT infrastructure for sharing financial data is one of the sensitive areas of services of general interest that fall within the scope of the EU NIS Directive. This is intended to ensure national and EU-wide resilience to hacker attacks and disruptions to security of supply so that consumers and society as a whole are not affected and harmed by network outages or data misuse. The planned systems are likely to be an extremely attractive target for attackers and should therefore be assessed in terms of data security. Against this background, it is surprising that network and data security are completely ignored. Common technical standards only concern interoperability. Financial data sharing schemes do have to define the contractual liability of the members if data security is compromised or the data is misused (in the case of personal data, the liability provisions are based on the GDPR). From AK's point of view, it is a shortcoming of the draft that it does not provide for any preventive measures against abuse. Furthermore, it is not clear whether attention is paid to GDPR-compliant data processing in third countries when setting up such sharing schemes. To date, banks have entrusted the international exchange of electronic information to the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Their use of US servers to store large amounts of sensitive payment transaction data for international transfers has been widely criticised.

AK concern: In light of the ECJ rulings on the illegality of data transfers between the EU and the USA based on various agreements such as the Privacy Shield and

standard contractual clauses, there is an opportunity to push for data storage within the EU. An obligation to store data on servers and clouds within the EU would be desirable.

Competent authorities

Member States should be free to choose the competent authorities only in so far as this does not affect the performance of data protection tasks. The latter are reserved to the data protection authorities, which should be explicitly pointed out in the draft. The enforcement tasks also include "to require, insofar as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of a breach and where such records may be relevant to the investigation of a breach of this Regulation".

Traffic data is subject to the communications secrecy of the ePrivacy Directive. As such, it can only be analysed for purposes other than billing under strict constitutional conditions. The European Court of Justice has already repeatedly rejected the "data retention" of traffic data for the purposes of criminal prosecution. Against this background, this data must be deleted after the connection has been established or, at the latest, after billing. In practice, there is therefore hardly any relevant leeway for a national access authorisation. The authorisation standard in the current draft also does not comply with the case law of the European Court of Justice, which requires precise specifications for encroachments on fundamental rights. Vague formulations such as "reasonable suspicion" or "may be relevant to the investigation" in no way comply with the principle of certainty and the principle of proportionality (only clearly defined, serious offences may be punished in this way).

AK concern: The data protection authorities are responsible for all data protection aspects of the regulation and must be explicitly named as such. The disclosure of traffic data (point vii) should be deleted without replacement due to a lack of conformity with the case law of the ECJ.

Contact us!

In Vienna:

Daniela Zimmer
T +43 (1) 501 65 12722
daniela.zimmer@akwien.at

Benedikta Rupprecht
T +43 (1) 501 65 12694
benedikta.rupprecht@akwien.at

Austrian Federal Chamber of Labour
Prinz-Eugen-Straße 20-22
1040 Vienna, Austria
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

In Brussels:

Florian Wukovitsch
T +32 (0) 2 230 62 54
florian.wukovitsch@akeuropa.eu

AK EUROPA
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54

www.akeuropa.eu

About us

The Austrian Federal Chamber of Labour (AK) is by law representing the interests of about 3.8 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore, the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectives of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Information from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.