EBF_046936

19 March 2026

EBF position on the European Commission's proposal for a Digital Omnibus Regulation – Data Act and GDPR

Executive Summary

The EBF recognises the efforts of the European Commission to modernise, simplify and strengthen the EU's digital regulatory framework, particularly in critical areas such as data and cybersecurity. Indeed, recent years have witnessed a growing inflation of digital regulation at European level, with often overlapping and contradictory requirements. The outcome of such normative inflation – as highlighted in the Draghi Report on EU Competitiveness - has been the creation of an increasingly complex, fragmented and at times excessively bureaucratic regulatory environment for businesses, with negative repercussions on their ability to compete and innovate.

The targeted adjustments proposed in the Digital Omnibus Regulation therefore represent a welcome first step towards simplification, helping in the creation of a coherent digital regulatory framework and making existing rules workable in practice.

While the proposed Digital Omnibus Regulation aims to capture the low-hanging fruits of simplification, more remains to be done. A **comprehensive assessment and stress testing of the impact of regulatory instruments** – horizontal vs. sectoral and digital vs. non-digital - **on the competitiveness of European firms is fundamental**. To this end, the upcoming Digital Fitness Check initiative should ensure sufficient coordination among different Directorate-Generals — particularly DG FISMA and DG CNECT for the financial sector.

In any case, any simplification effort should not translate into deregulation nor the weakening of fundamental rights. Rather, it should aim to:

1) **Enhance legal clarity**, by addressing grey areas and eliminating overlaps and inconsistencies in regulatory requirements that hinder effective interpretation and implementation;
2) Ensure **harmonization of application** between member states, as differences in practice across member states have created a very complex environment for companies operating in multiple member states. This also represents an obstacle for further integration of the Single Market, and
3) **Streamline administrative processes**, enabling companies to better anticipate and fully comply with their obligations, while focussing resources on core activities, rather than demonstrating tick-box compliance.

This paper presents the EBF's contribution to the Commission's simplification effort. It highlights welcomed proposals, identifies areas for further improvement, and outlines additional opportunities to streamline the EU data acquis, with a view to enhancing its overall effectiveness, coherence and predictability necessary to support sound implementation, innovation and competitiveness.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

Key EBF Messages and Recommendations by Area

Data Act: We welcome the proposal to bring together all concepts and principles for non-personal data sharing under a single regulation, improving harmonisation at European level.

- **Market-based compensation**: The calculation of reasonable compensation to the data holder should be based on a market-based valuation logic, taking into account the investments made by the data holder and the possibility to include a margin.
- **Exemption criteria**: Exemptions from data-sharing obligations under the Data Act should not be based solely on company size, but also on other criteria, such as the volume of data processed.

GDPR:

- **Definition of "personal data" (Art. 4(1))**: The proposed amendment to the definition of personal data raises several fundamental legal and practical questions, and as such, may fail to offer the legal certainty expected by stakeholders.
    - **Recommendation**: **The debate around re-identification should be moved out of the fast-track Omnibus Simplification process**.
- **Processing of special categories of data for AI development/operation (Art. 9(2)(k) and 9(5))**: We **welcome** the possibility to use special categories of data that residually exist from AI training/operation as defined in the AI Act.
- **Processing of biometric data for identity verification (Art. 9(2)(l))**: we welcome the introduction of a derogation allowing the processing of biometric data for identity verification under the sole control of the data subject, if the co-legislators take the view that this does indeed amount to the processing special categories of personal data.
- **Limits on abusive or excessive data access requests (Art. 12(5))**: We **support the proposal to better address unfounded or excessive data access requests**. This ensures that that banks can focus on genuine access requests and shield themselves against the growing volume of abusive or strategically motivated requests.
    - **Recommendation**: **Clarify**, by way of a Recital, that the requirement on controllers to comply with **a data access request is limited to providing a copy of the personal data undergoing processing** and does not extend to the provision of the associated documentation.

- **Automated Decision Making (Art. 22)**: While welcome the intention of the Commission to move away from the prohibition on automated decision making, **phrasing such permission only in specific circumstances still resonates as a prohibition with an exception regime**.
    - **Recommendation**: **Clarify that, whenever a controller takes a decision based solely on automated means which produces legal or similarly significant effects for a data subject, the use of automated decision-making – irrespective of the legal basis – must be accompanied by the implementation of appropriate safeguards** (e.g., human intervention).
    - **Recommendation**: Clarify that controllers are not obliged to disclose internal algorithms, proprietary logic, or commercially sensitive business knowledge as part of their information obligations.
- **Notification of personal data breaches to DPAs (Art. 33)**: We **welcome** the Commission's proposal to **focus** notification duties on personal **data breaches that are likely to result in a high risk** to the rights and freedoms of individuals and to **extend the notification to 96 hours**.
    - **Recommendation: Align the calculation of the notification period with Regulation No 1182/71**, expressing time limits in working days.
    - **Recommendation:** Allow controllers to record and treat low-risk incidents as operational incidents as opposed to formal data breaches.
- **Access to terminal equipment (Art. 88a and 88b)**: We generally **welcome** the proposal to have a **single, unified framework regulating the processing of personal data in the terminal equipment of natural persons under the GDPR**.
    - **Recommendation**: **Clarify that Article 88a(3) takes precedence over Article 6(1)(f)** for processing activities covered by it.
    - **Recommendation**: **Delete Article 5(3) of the ePrivacy Directive** to avoid the creation of two different legal regimes for personal and non-personal data.
    - **Recommendation**: **Delete Article 88b(6)**. In practice, browser providers are almost exclusively non-European and at the heart of the online advertising value chain, which raises significant legal, technical and strategic questions.

1. Amendments to Regulation (EU) 2023/2854 ("*Data Act*")

The Digital Omnibus proposes to integrate all the principles and concepts of the various legislative instruments on non-personal data – the DGA, the ODD and the FFDR – into the Data Act, making the latter the single reference regulation for data sharing. As we understand it, the amendments will consolidate B2C, B2B, B2G, and Open Data data-

sharing requirements, and incorporate and clarify the concepts of data intermediation services into the Data Act.

This simplification measure is welcome insofar as it makes the reading and analysis of requirements relating to data sharing and re-use – both public and private – clearer. Having a single regulation bringing together all concepts and principles for data sharing, and serving as the foundation for sectoral regulations, further improves harmonisation at European level. However, further work to clarify definition – particularly that of data holders – and reinforcing horizontal principles of data sharing is necessary.

1.1. Horizontal Principles of Data Sharing

1.1.a - The Principle of Compensation

Access to a company's data cannot be free of charge, especially where the data constitutes strategic assets in which investments have been made (for data collection and processing), and where access relies on a service that is costly to provide.

A value-sharing mechanism based on reciprocity is essential both to foster innovation and to encourage data holders to invest in data standardisation. **Reasonable compensation should therefore not be defined at a minimum level; rather, the calculation method should be based on a market-based valuation logic** so as not to undermine the competitiveness of data holders. This should take into account the costs incurred for making the data available (including the collection, generation, structuring, preparing, and sharing of the data), and the investment in the collection and production of data (in addition to the costs for making the data available), which should include a margin.

1.1.b - Intellectual property rights and trade secrets

Maintaining the protection of intellectual property, trade secrets and data that are sensitive and strategic for businesses is essential, and excluding such data from mandatory data sharing is necessary to preserving the competitiveness and sovereignty of European companies. In this regard, Article 1(3) of the Digital Omnibus, which provides new grounds for refusing the sharing of sensitive data, is welcome. Under the Data Act, data holders could refuse to disclose trade secrets where they consider there to be a high risk of unlawful disclosure to entities subject to foreign jurisdictions that do not offer an equivalent level of protection.

More generally, the European Commission's intention to strengthen the international competitiveness of European companies by reducing financial losses and reinforcing the protection of know-how – as an expression of the fundamental freedom to conduct a business – can only be welcomed.

1.2 - SMEs exemptions from certain data-sharing obligations

The Digital Omnibus provides exemptions for micro and small enterprises, as well as mid-sized companies, from certain data-sharing obligations. While simplification challenges are particularly significant for small businesses, this must not lead to distortions of competition. Such exemptions must not run counter to the principle of equal treatment.

We would like to recall that, on the one hand, the value and sensitivity of data are not proportional to the size of a company. On the other hand, certain actors – such as payment data aggregators – are small companies that nevertheless process very large volumes of data, which can be highly sensitive. From a competition and data protection perspective, exempting micro and small enterprises would not be justified and could even prove

counterproductive. We believe the volume of data processed should also be taken into account, and not only the size of the company.

---

2. Amendments to Regulation (EU) 2016/679 ("*GDPR*")

The GDPR plays a crucial role in safeguarding personal data within the EU, and its introduction has resulted in a significant increase in the attention for and application of data protection rules. However, complexities in its application and implementation hinder efficient compliance and processing, which are particularly acute for highy regulated sectors, such as banking, and for companies operating cross-border. For example, diverging national enforcement practices, especially among data protection authorities, have led to legal uncertainty, compliance inefficiencies and regulatory arbitrage, undermining the functioning of the single market (one of the largest trade areas of the world), particularly in cross-border financial services1. Additional challenges arise from the growing number of sector-specific legislation that require the processing of personal data and the difficulty of reconciling seemingly conflicting principles on which these acts are based. In particular, tensions emerge between GDPR principles (e.g., data minimisation) and sectoral European or national frameworks, such as those regulating anti-money laundering, payments, and credit risk management. This is further aggravated by conflicting guidance from regulators, placing banks in a complex and sometimes contradictory compliance position. The differences among Member States in the implementation and enforcement of the GDPR also creates risks for European companies from being excluded from early innovations (with negative impacts on competitiveness) because of uncertainty, complexity and fragmentation of regulatory frameworks.

Against this background, we welcome the Commission's overarching goal to reduce the administrative burden for EU companies, including banks, and better align the GDPR to the EU's Digital Agenda.

2.1 - Amendment to Article 4(1) and new Article 41a – Definition of "personal data" and criteria to determine "*unidentifiable*" pseudonymised data

The proposed amendment seeks to clarify, in light of the Court's judgment in Case C-413/23 P, that information would not be considered personal data for an entity when it does not have the "means reasonably likely" to identify the natural person to whom the information relates. While we welcome the Commission's intention to clarify the complex issue of defining what constitutes "personal data", this amendment raises several fundamental legal[2] and practical questions (e.g., contractual governance, technical

---

1 This was confirmed in the European Commission's second report on the implementation of the GDPR, where market participants indicated the following:

- there are often divergent views on whether an entity is a controller or processor;
- in some cases, DPAs do not follow the EDPB guidelines at national level; and
- these problems are exacerbated when multiple data protection authorities within the same Member State adopt conflicting interpretations.

[2] Remaining open question include:

- The relevant perspective for assessing identifiability in different scenarios;
- The notion of "means reasonably likely to be used";
- The extent to which controllers can implement measures to limit the means "reasonably likely" to be used for re-identification;

compliance) that warrants careful consideration. Given the complexity and sensitivity of the issue – touching on the very concept of personal data and thus on the applicability or not of the GDPR – **we recommend that the debate around re-identification is moved out of the fast-track Omnibus Simplification process**, as the amendment, as currently drafted, may fail to offer the legal certainty expected by stakeholders, potentially leading to unforeseen and adverse outcomes. Instead, **we call on the European Commission to engage with all relevant stakeholders - including IT, security and technology experts - to develop a robust framework around re-identification that, in a pragmatic approach, ensures the most appropriate level of protection for personal data taking into account ongoing technological advancements in our global open data (risk) landscape**.

2.2 - New Article 4(38) - Definition of "*scientific research*"

The GDPR refers to the notion of "scientific research" in several provisions (e.g., Articles 5(1)(b) and (e), 9(2)(j), 14(5)(b), 17(3)(d), etc.), despite the fact that the term is not legally defined in the text of the GDPR itself. The proposed introduction of a definition of "*scientific research" under* Article 4(38) is therefore a welcome addition, as it clarifies when the specific provisions of GDPR regarding "scientific research" can be applied, including for research activities pursued with a view to furthering a "commercial interest".

2.3 - New Article 9(2)(k)-(l) and 9(5) - Special categories of data in the context of AI development/operation and the use of biometric data

We **welcome the possibility to use special categories of data that residually exist in the training and operating of AI systems,** as defined in the AI Act. This change also closes the gap between the GDPR and Article 10(5) and Recital 70 of the AI Act, with the latter allowing the processing of special categories of data to prevent or correct algorithmic bias in relation to high-risk AI systems, based on substantial public interest, provided that strong safeguards are in place[3].

For legal certainty and consistent enforcement, however, we would welcome further clarification on the following elements:

- **Clarification** – in the form of Guidelines – **of concepts such as "*effectively protect*"** (Art. 9(5)) would be useful, for example by recognising standard privacy-enhancing technologies (e.g., tokenisation, access controls, model governance)

- The associated implications for data processing under Article 28 (e.g., the controller's decision-making authority, rights of disposal and instruction).

3 Article 10(5) AI Act: "*To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued*."

Recital 70 AI Act: "*In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should, exceptionally, to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons and following the application of all applicable conditions laid down under this Regulation in addition to the conditions laid down in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, be able to process also special categories of personal data, as a matter of substantial public interest within the meaning of Article 9(2), point (g) of Regulation (EU) 2016/679 and Article 10(2), point (g) of Regulation (EU) 2018/1725*."

and other AI privacy-enhancing technologies (e.g., Differential Privacy or Federated Learning) as appropriate safeguards in this context;

- **Guidance on the related safeguards**, with a view to ensuring that they remain proportionate and do not result in a limitation to the practical applicability of the derogation.

We also welcome the introduction of a derogation allowing the processing of biometric data for identity verification purposes under the sole control of the data subject, for this can support with secure digital onboarding and authentication. However, to further ensure legal certainty and consistent obligations where AI and data protection provisions intersect, **clarification should also be provided on the following elements: (1) the scope of the definition of "biometric data" under the GDPR and the AI Act; (2) the difference between "*verification*" and "*unique identification*"; and (3) the wording "*under the sole control of the data subject*"**.

(1) Definition of "biometric data"

We note that there is a mismatch in how the GDPR and the AI Act define "biometric data".

Article 4(14) GDPR	**Article 3(34) AI Act**
(14) biometric data means "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data."	(34) biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopy data".

From the table above, it emerges that the definition of biometric data under the AI Act does not include the notion of "unique identification" found in the GDPR definition. As a result, the definition of biometric data in the AI Act can be considered broader than the one provided by GDPR, since it does not require that the biometric data allows or confirms the unique identification of a person.

This difference between the two definitions is also highlighted in the Commission Guidelines on prohibited artificial intelligence practices. As part of their upcoming Guidelines on the Interplay between the GDPR and the AI Act, we recommend that **the EDPB and the AI Office clarify the scope of application of the term "biometric data" across the two legislative frameworks. This is necessary to ensure legal certainty, clarity of legal interpretation and of controllers' obligations.**

A direct consequence of the differences in definitions of "biometric data" and their scope is **unclarity as to what falls under "special categories of data" mentioned in Article 10(5) AI Act**[4]. While under the GDPR, biometric data qualifies as a special category of data only for the purpose of uniquely identifying a natural person, Recital 54 of the AI Act appears to treat biometric data as a special category by default ("*As biometric data constitutes a special category of personal data (...)*"). The question that arises is

4 Article 10(5) AI Act: "To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons."

whether the broader interpretation of "biometric data" under the AI Act still falls within the "special categories of data" of the GDPR, in cases of processing that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems. **Clarification from the EDPB and the AI Office on this point is necessary.**

(2) ***"Verification" vs "unique identification"***

We also urge co-legislators to establish a common understanding on the concepts of "*verification*" and "*unique identification*" in the context of biometric data processing. In our view, the GDPR is clear on when biometric data qualifies as a special category of data – namely, when it is processed to uniquely identify a data subject, which is based on a "one-to-many" comparison of the data subject's biometric data against a database. Verification, on the other hand, as expressly recognised in the new Recital 34, "*is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity*."

We also note that, from the perspective of the banking sector, identity verification constitutes a legitimate purpose for processing, as well as a legal obligation during remote onboarding and servicing, and represents one of the main reasons banks process biometric data. In this context, we can distinguish between two purposes:

1) First, the processing of biometric data to understand whether a person is the duly authorised/verified customer that is being serviced within an established relationship with the bank. An example of this is the use of a fingerprint to unlock/authorise access to the banking app instead of a password. Here, the system compares the biometric sample to a stored template linked to that specific user account. Similarly, facial recognition may be used in a branch setting to double-check the identity of the customer being services – for instance, when executing large transactions - instead of a manual check. In this case, the processing answers the question: "*Is this the same person who previously registered this account?*".
2) Second, the processing of biometric data in situations where the bank needs to verify a new customer's identity during remote onboarding and confirm that the person presenting an ID or passport is the legitimate document holder. In this case, the system checks that the face matches the ID/passport photo - a 1-to-1 verification. It answers the question: "*Is this person the legitimate holder of this ID?*".

Building on these considerations, a 1-to-1 verification does not amount to "*uniquely identify a natural person*" ("*1-to-many*").

If the co-legislators share these same views, then the proposed derogation may not be necessary, because only when biometrics are used to uniquely identify a person the processing of special categories of data takes place. From a legislative technique perspective, **our preference would therefore be not to introduce the exception to Article 9, but rather to clarify in the recitals that verification of a data subject's identity as a result of processing of biometric data does not amount to the processing of special categories of data**.

However, if the co-legislators take the view that 1-to-1 verification does indeed amount to the unique identification within the meaning of Article 9 GDPR, the introduction of an explicit exception is welcome.

2.3.1 - Additional recommendations regarding the exceptions to use special categories of personal data

We would also like to propose the following additional recommendations to Article 9 GDPR.

Amendment to Article 9(2) GDPR to include processing necessary for the conclusion and performance of a contract

We propose to allow for the **processing of special categories of data under Article 9(2) based on processing necessary for the conclusion and performance of contracts**. This would provide a necessary and workable framework for banks to legitimately process customers' sensitive data where such data is inherently linked to the execution of financial services. In the banking sector, this is particularly relevant in the following instances:

- **where the data subjects are incapacitated to express consent** (e.g. information about a limited legal capacity, disability benefits, long-term illness causing delays in credit repayment). Being able to process this information on the basis of contract execution is essential to deliver appropriate services and meet customers' needs but also in better supporting banks in complying with accessibility legislation, by allowing them to provide clients with disabilities access to banking services appropriately tailored to their specific needs (e.g., recognising that a client with speech impairment will not be served via phone, delaying a credit payment due to the client's illness).
- In cases of "**accidental/incidental processing**", that is when special categories of data appear incidentally in transactional data carried out by the customer through the current account or debit/credit cards or even included in the reasons for the transfers. An example is the free-text field in a wire transfer, where customers sometimes include sensitive information (e.g. "payment of medical expenses for surgery", "contribution to parish HIV fund", etc.) or payments to medical institutions or doctors from which health data can be indirectly derived. In such cases, the bank must process this data to execute the payment, which is purely incidental to fulfilling the contractual obligation. However, as the payments framework currently stands, the accidental/incidental processing of special categories of data cannot rely on the PSD2 legal basis. PSD2 processing is grounded in contractual necessity, which cannot be relied upon when the processing involves, even if fully incidentally, sensitive categories of personal data.

Overall, the processing of special categories of personal data through the contract-based legal basis would allow financial institutions to continue operate effectively and responsibly, including in areas such as insurance and daily banking, where the processing of such data is often unavoidable.

Amendment to Article 9(2)(e) GDPR to include processing related to personal data manifestly made public by the data subject

In banking, customers often voluntarily share sensitive information seeking favourable decisions, such as debt restructuring due to hospitalization. Processing such information is vital for making decisions that benefit the data subject, ensuring their needs are met

effectively. However, these data, which are being voluntary provided by data subjects, do not qualify as "data manifestly made public" under Article 9(2)(e) nor do they meet the explicit consent criteria under Article 9(2)(a).

To cater for these situations, **Article 9(2)(e) should be clarified to include instances where the data subject voluntarily provides sensitive personal data**. This exemption to Article 9(1) should also extend to obvious health-related issues—such as physical disabilities—enabling banks to collect and process such information to offer accommodations of accessible spaces.

Amendment to Article 9(2)(h) GDPR to access special categories of personal data without consent

Article 9(2)(h) states that specific consent is not required for processing of special categories of data for the purpose of "the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional". This provision should be expanded to include other purposes, such as verifying such data for contingencies related to financial products like pension funds.

Amendment to Article 9(1) GDPR to limit special categories of personal data to data that is "directly" linked to a data subject

The sector support reinstating the proposed amendment included in the leaked version of the Commission's proposal – namely limiting the concept of special categories of personal data so that it only applies to data that "***directly reveals in relation to a specific data subject (…)***", as opposed to the current broad wording ("*revealing*"). This clarification would reduce uncertainty about what is covered and provide better predictability, e.g., when processing transaction data.

2.4 - Amendment to Article 12(5) - Limitations to the right of access in case of abusive or excessive requests

We support the proposal to better address unfounded or excessive data access requests, while maintaining the principle that exercising data subject rights should remain free of charge in ordinary cases. The growing volume of abusive or strategically motivated access requests places a significant operational burden on banks, and this amendment - by lowering the threshold for demonstrating that a request is unfounded - ensures that that banks can focus on genuine access requests and defend themselves against requests intended to cause damage or harm.

To support a harmonised approach across Member States, EU-level guidance with concrete examples of abusive or excessive behaviour would be beneficial, so that controllers and supervisory authorities apply a comparable threshold in practice. Similarly, further clarification would be helpful as to how controllers are expected to demonstrate, in practical terms, a data subject's intention to cause damage or harm to the controller (cf. Recital 35).

We also recommend clarifying, by way of a Recital, that **the requirement on controllers to comply with a data access request is limited to providing a copy of the personal data undergoing processing and does not extend to the provision of the associated documentation**, as required by some national DPAs. Such interpretation exceeds the scope of the data subject's right of access and imposes a disproportionate administrative burden on companies. This was also confirmed by the EDPB in its guidance on the right of access[5].

We also recommend **clarifying directly in Article 15 (not just by way of Recital 63) that the right of access may only be used by the data subject to pursue their data protection rights and not for any other purposes (purpose limitation)**. While the right of access of the data subject under Article 15 GDPR is a cornerstone of data protection law - as confirmed by the case law of the CJEU, in practice and as acknowledged in the case law (see ECJ, judgment of October 26, 2023 - C 307/22), this right is also being exploited to an excessive degree for purposes unrelated to data protection (e.g., in labour law disputes over termination in the context of negotiations on severance payments).

Finally, **we also recommend extending this proposal to tackle abuses of data access rights to cover all rights under the GDPR**. This would give controllers a clear and legally secure means/threshold to handle abuses of rights across the board.

2.5 - Amendment to Article 13(4) - Proportionate transparency for low-intensity processing

We welcome the creation of a simplified information regime for situations with a clearly defined relationship between data subject and controller, low data intensity and a reasonable expectation of being informed, as a pragmatic way to reduce "information fatigue" in low-risk cases. To avoid divergent interpretations, further operationalisation of notions such as "*not-data intensive*" and "clear and *circumscribed relationship*" would be beneficial.

Regarding the waiving of the controller's obligation to inform data subjects about the processing of personal data in situations where there are reasonable grounds to assume the data subject already possesses the information, **confirmation should be provided that such knowledge can be presumed when the information is provided in the policy or made available on the entity's website, and when the data subject/customer is the direct source of the data**.

2.6 - Amendment to Article 22 – Automated Individual Decision Making (ADM)

In its AI Continental Action Plan, the European Commission set out the EU's path towards widespread development and adoption of AI solutions, aiming to boost competitiveness in full respect of fundamental rights. This reflects a wider trend towards greater digitalisation and AI deployment across key sectors - including finance – which is inevitably leading to an increased use of automated decision-making (ADM) in the everyday processes of banks.

---

[5] European Data Protection Board, Guidelines 01/2022 on data subject rights - Right of access, *"(…) the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents (see section 5, para. 152). More generally speaking,* ***there is no additional information to be given to the data subject upon providing a copy****: the scope of the information to be contained in the copy is the scope of the access to the data under 15(1) (second component of the right of access as referred to above, see para. 19), which includes all information necessary to enable the data subject to understand and verify the lawfulness of the processing."* (par. 23).

We therefore welcome the intention of the Commission to move away from the prohibition on automated decision making towards the creation of a framework that defines conditions under which automated decisions are permitted[6], consistent with the realities of modern financial services. We note, however, that **phrasing such permission only in specific circumstances** ("*may be based solely on automated processing […]* ***only where that decision****: …*") **still resonates as a prohibition with an exception regime. Instead, it should be clarified that, whenever a controller takes a decision based solely on automated means which produces legal or similarly significant effects for a data subject, the use of automated decision-making – irrespective of the legal basis – must be accompanied by the implementation of appropriate safeguards**. These safeguards should include the right to obtain human intervention, the right of the data subject to express his or her opinion and to contest the decision; and where a data protection impact assessment (DPIA) identifies the need for additional measures, those measures should also be duly implemented. This will ensure that, whenever a bank takes a decision through automated means that affects a data subject, safeguards will always be in place.

In addition, to provide full legal certainty after recent case law, further clarification of the following would be helpful:

- The "necessity" requirement and the notion that a decision can be taken "*regardless of whether the decision could be taken otherwise than by solely automated means*". This wording is not clear and should be further illustrated. In particular, it should be clarified directly in the text of the GDPR that the mere fact that the decision could also be taken by a human does not prevent the controller from taking that decision through solely automated processing. At the same time, is should be clarified that, when several automated processing solutions exist, the controller should use the less intrusive one for the data subject;

- **Transparency obligations regarding the logic of ADM**: it would be helpful to **confirm**, by means of a Recital, that **the requirement to provide "*meaningful information about the logic involved*" does not oblige controllers to disclose internal algorithms, proprietary logic, or commercially sensitive business knowledge** (in line with the CJEU interpretation in case C-203/22). Transparency should focus on enabling data subjects to understand the nature of the decision being taken, the categories of data used, and the potential consequences, rather than exposing the underlying model architecture or trade secrets (please also refer to the section 2.11 for a more details overview of transparency obligations in the context of automated decision making).

- **Processing of special categories of personal data**: **ADM involving Article 9 data should also be permitted when strictly necessary for contract initiation or execution, and when sufficient safeguards are in place**. This is especially relevant in insurance contexts, where the use of special category data may be inherent to risk assessment and underwriting.

2.7 - Amendment to Article 33 - Notification of a personal data breach to the supervisory authority

6 Article 14 of the AI Act expressly provides that high-risk AI systems can be used, provided that they are designed and developed subject to human oversight throughout their life cycle. By contrast, the current text of the GDPR imposes a blanket prohibition on ADM (including non-high-risk ones), marking a clear departure from the risk-based approach of the AI Act.

We **welcome the Commission's proposal to focus** notification duties on personal data breaches that are likely to result in a **high risk to the rights and freedoms of individuals** and to **extend the deadline for notification from 72 to 96 hours**. This goes in the right direction of simplifying procedures, allowing more time for controllers for fact-finding, containing damages and minimizing risks, and involving authorities when their intervention is of essence, as their mission is to end the risk to the data subjects as quickly as possible through official counselling.

We highlight, however, that from a practical and legal-certainty perspective, an hour-based deadline remains problematic, especially for incidents that occur on Fridays or immediately before public holidays. In such constellations, controllers are often forced to submit incomplete or weakly substantiated notifications merely to avoid missing the deadline. **We therefore suggest aligning the calculation of the notification period with Regulation No 1182/71**[7], expressing time limits in working days (as opposed to hours) and automatically rolling over a deadline expiring on a Saturday, Sunday or public holiday to the next working day. This would enable controllers to comply with the legal requirements while ensuring that investigations and internal clarifications can be carried out with the necessary quality.

If co-legislators don't find not feasible, then the 96-hour deadline should instead be defined in business hours, which would provide companies with a greater margin of action.

Finally, **further meaningful and practical simplification of GDPR obligations could be achieved by allowing data controllers to record and treat low-risk incidents as operational incidents as opposed to formal data breaches**. We note that in practice, most controllers notify their DPA of none or only 1 to 2 data breaches per year. At the same time, controllers experience "low risk" data breach cases almost daily, the vast majority of which arise from human errors (for example, misdirected emails within the organisation). Formally registering and managing all these cases as data breaches triggers the same internal procedures required for currently defined "risk" and "high risk" data breaches – namely, registration, investigation, decision-making, documentation - and requires the mandatory involvement of at least 3 to 4 specialists. While controllers should continue to collect information about such opreational incidents, applying the full set of requirements foreseen for high-risk data breaches to low-risk incidents creates a significant administrative burden for controllers while offering limited practical benefit to data subjects.

2.8 - Amendments to Article 35 – DPIA

We welcome the proposal of establishing EU-wide black/whitelists of processing operations requiring a DPIA, as this can reduce national fragmentation and provide more predictability for cross-border business models. We would encourage a clearly risk-based calibration of the list.

Another area where clarification is fundamental to facilitate compliance of the private sector and ensure comprehensive protection of data protection rights is the relationship and interplay between the Data Protection Impact Assessment (DPIA) under the GDPR and the Fundamental Rights Impact Assessment (FRIA) under the AI Act.

Pursuant to Article 35 GDPR, a Data Protection Impact Assessment (DPIA) is to be carried out for data processes that are likely to yield high risks to the rights and freedoms of

7 Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits http://data.europa.eu/eli/reg/1971/1182/oj

natural persons The AI Act, on the other hand, requires deployers of high-risk AI systems to carry out a Fundamental Rights Impact Assessment (FRIA) to assess the impact/risks that such systems may have on an individual's fundamental rights.

From the above, it is clear that the main difference between a DPIA and a FRIA is the scope, in that the FRIA goes beyond the DPIA's, focusing on a more comprehensive evaluation of fundamental rights beyond data protection. However, the two impact assessments share many key features, including an ex-ante procedural approach and a rights-based focus on risk assessment. This common nature is explicitly recognised in Article 27(4) of the AI Act, which combines the FRIA and DPIA in their common areas: "*If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 (...), the fundamental rights impact assessment(...) shall complement that data protection impact assessment.*"

This makes a comparison between the two tools essential, as they **share similar purposes in risk management, but apply in different contexts, with the DPIA focused on the protection of personal data and the FRIA extended to all fundamental rights in the context of AI**.

In conclusion, we may assume that in those cases in which high-risk AI systems process personal data, the DPIAs carried out on such personal data processing will cover part of the requirements associated with the FRIA and, therefore, the performance of the FRIA should cover those areas required by the AI Act that have not been assessed in the DPIA. **The relationship between the DPIA and FRIA should be made more explicit in the GDPR; this can be done by including a specific reference to Article 27 of the AI Act in Article 35 of the GDPR** (or alternatively, in the recitals).

As the two impact assessments will co-exist, their coordination in terms of content and methodology is also necessary. In this regard, we note that the AI Office is expected to develop a FRIA template helping deployers of high-risk AI systems to comply with their obligations under Article 27 of the AI Act. **To avoid redundant assessment processes and the duplication of administrative efforts that could arise due to overlapping requirements in the two assessments, we recommend that the AI Office, in cooperation with the EDPB:**

- **Ensures, to the greatest extent possible, a substantive and structural integration of the DPIA and FRIA, aligning methodologies while preserving their distinct legal bases and objectives;**
- **Clarifies that, ultimately, controllers/AI deployers should have the freedom to choose which methodology to adopt when performing a FRIA and DPIA assessment** for AI systems processing personal data based on their internal structure and processes already in place.

2.9 - New Article 88a and 88b - GDPR and the ePrivacy Directive

We generally **welcome the proposal to have a single, unified framework regulating the processing of personal data (in particular the storing and access) in the terminal equipment of natural persons under the GDPR**. It is however important that all relevant processing activities are covered; in this regard, the terms "storage" and "access to already stored" personal data risks being too narrow, particularly in those cases where digital tracking does not involve directly identifying a person.

Similarly, while we understand this to be the intention of the Commission, we see the need to **clarify in a Recital that Article 88a(3) takes precedence over Article 6(1)(f) for processing activities covered by it**, so that controllers do not need to carry out a balancing test or handle objections under Article 21(1) for such processing.

Moreover, **to enhance the security of users and banking customers, we strongly suggest including, under Article 88a(3), an exception to the requirement for consent** for any storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person and subsequent processing **aimed at preventing the misuse of the online service, combating fraud, money laundering, and terrorist financing**. The use of these technical procedures for the prevention of misuse and fraud should continue to be possible without consent (this would also be in line with Recital 47 GDPR, which recognises fraud prevention as falling under the legitimate interest ground).

Article 88a(4)(a) requires data controllers to allow users to refuse consent with a single click. In order to preserve methods of obtaining consent that are well-established in practice and recognized by European and national legal regulators, and to avoid making obtaining consent more complex than refusing to give it, it is **necessary that this new provision also allows users to give their consent with a single click**.

We would also like to share the following observations on the prohibitions on repeating a request for consent under **Article 88a(4)(b) and (c)**:

- It should be noted **that if a user deletes read or write operations on their browser's terminal**, either manually or automatically at regular intervals**, the controller is no longer technically able to determine whether or not the user has given consent to these operations**. Therefore, in this case, it is **necessary to allow the controller to request the user's consent again within a period shorter than six months**.
- We would welcome a clarification of the minimum data points that controllers may retain for verification purposes.

We also highlight more broadly that, while Article 88a is welcome, this proposal will *de facto* lead to the creation of two different legal regimes and rules for personal and non-personal data, under the GDPR and the ePrivacy respectively. We therefore **question the need to retain Article 5(3) of the ePrivacy Directive, both in light of the boundary issues arising in relation to the new Article 88a GDPR and in terms of the values the provisions seek to protect when it no longer concerns personal data. We therefore recommend deleting Article 5(3) from the ePrivacy**, as the value proposition of the provision – after the introduction of Article 88a GDPR – may otherwise be legitimately questioned.

Finally, under the new Article 88b, the Digital Omnibus proposes allowing users to give and refuse consent at the browser level. In practice, we note that browser providers are almost exclusively non-European and at the heart of the online advertising value chain. Delegating consent collection to these companies raises significant:

- legal questions (e.g., issues of conflicting laws, data transfers, and compliance monitoring of the companies involved);
- technical questions (e.g., proliferation of international intermediaries); and

- strategic questions (e.g., challenges to European sovereignty, technological dependence, and delegation of the exercise of a right intimately linked to the fundamental right to privacy).

From a banking perspective, additional challenges arise. Unless a client has logged into their online bank account, it is not possible to identify the client at a browser level. Nor it is possible to determine whether consent has been provided by a minor or by one user of a shared device (for example, a family laptop), thereby binding all other users of that device.

In light of these concerns, **we recommend deleting Article 88b(6).**

2.10 - New Article 88c - Processing in the context of the development and operation of AI

While we appreciate the Commission's effort to codify in the text of the GDPR the possibility to rely on legitimate interest under Article 6(1)(f) GDPR as a legal basis to develop and operate AI systems, we would like to make the following observations:

- in practice, it is already possible to rely on this ground for such purposes;
- the risk-based approach of the GDPR already grants controllers discretion over the most appropriate legal basis for processing, taking into account the nature of the processing activities and the safeguards implemented;
- the GDPR does not prohibit the choice of a legal basis on the grounds of the technology involved; and
- From a future-proofing perspective and to maintain the tech-neutral approach of the GDPR, it may not be appropriate to have a specific legal basis for every new technology that emerges.

2.11 - Additional EBF proposals for GDPR Simplification

In addition to the amendments proposed by the European Commission, the sector would like to contribute to the simplification efforts by suggesting additional targeted amendments to the GDPR that serve the purpose of:

1. **Streamlining and harmonising provisions** that would otherwise be subjected to differential interpretation and that require agreement across Member States; and
2. Better **aligning the GDPR to the EU's Digital Agenda**.

A. Article 6 – Legal Bases for processing personal data

The banking sector relies on different legal bases to process personal and special categories of data, on the basis of the purpose of the processing, as well as the category of personal data involved.

Nevertheless, because the grounds for processing have been designed to be sector-agnostic and apply to a wide range of data controllers/processors:

- uncertainty arises when determining which legal ground should be relied on, particularly when applied to sector-specific circumstances;
- legal ambiguities may arise that obstruct efficient data processing that pose no threat to data subjects' rights and freedoms.

Clarifying Legal Obligations vs. Legitimate Interest under Article 6 GDPR

In heavily regulated sectors like the banking one, **distinguishing between legal obligations and legitimate interests is crucial due to varying specificity in laws across countries**. This differentiation is essential as these legal grounds trigger distinct rights and obligations. For instance, data subjects can object to processing based on legitimate interests but not when it's based on legal obligations.

When relying on Article 6(1)(c), laws allowing to process personal data often lack specificity on the legal basis to be relied on (i.e., legal obligation) as they don't spell out the specific purpose for processing and complete instructions on the categories of personal data that should be included in the process (this is the case for example, when there is a legal obligation to manage conflicts of interest or manage ICT risk). We also observe that many national DPAs refuse reliance on Article 6(1)(c), on the grounds that the law must provide greater detail and specificity on the type of data to be processed, retention periods, etc. Thus, as this specificity is required in principle to process data based on a legal obligation, the lack thereof renders the legal basis null and void. Controllers are thus left to processing under Article 6(1)(f) (legitimate interest) to comply with a statutory duty, which requires an additional Legitimate Interest Assessment (LIA), adding further burden on controllers. At the same time, there appears to be a growing tendency - or at least an implicit expectation - from supervisors to treat their guidelines or decisions as akin to a legal obligation, as opposed to recommendations, bringing further uncertainty in practice.

In those instances where core activity processing can rely on the ground of a legal obligation, many sectoral laws impose duties on banks (e.g. AML, prudential supervision) without spelling out every accessory processing step needed to fulfil those duties. In practice, this means that all accessory or enabling processing (data quality checks, record management, internal reporting) must be shifted to legitimate interest, triggering additional balancing tests and objections. This creates a situation whereby one regulatory duty is fragmented into multiple legal bases, creating unnecessary complexity and weakening legal certainty.

A new recital in the GDPR - or an addition to Recital 41 - explaining the relationship between the two grounds would be welcome; if not feasible, then clear guidelines (for example, under the draft EDPB Guidelines on Legitimate Interest) on when to apply a specific legal basis versus another would help streamline compliance efforts and ensure consistent application of GDPR provisions, aligning with both regulatory requirements and business operations. Specifically, the sector would welcome if the co-legislators could clarify the following aspects:

- The controller may rely on a legal obligation as a legal basis of processing when processing is supported by a legal act (even when the latter does not specify in detail the exact categories of data, the scope and modalities of data processing, etc.) or supervisory guidelines. Entities should not be required to conduct an additional legitimate interest assessment;
- Accessory or ancillary processing directly linked to a legal duty may also be considered covered by Article 6(1)(c). For example, when the law requires banks to monitor for AML, all necessary data operations to make that monitoring effective (e.g., screening, enrichment, alerts management,

model validation, etc.) should fall under "legal obligation", when the underlying duty is statutory, even if not expressly named in the latter. Only genuinely separate or additional processing should require another legal basis.

B. Data Subject Rights

Waiving Right to Object Under Article 21 GDPR when processing is based on Article 6(1)(e) GDPR

Any processing based on Article 6(1)(e) stems from EU or member state laws that authorize the carrying out of a task in the public interest. We assert that when processing serves the public interest, its legitimate grounds are inherently compelling. This is the case of AML requirements, which some jurisdictions recognise as falling under public interest given the wording in the AMLD that fight against money laundering serves the public interest. Consequently, the right of data subjects to object against a legal obligation becomes largely formalistic, as outcomes of such objections are predetermined by legal mandates approved by the state.

Waiving this right acknowledges the practical realities and ensures smoother operations without undermining data subjects' rights unnecessarily. It aligns the GDPR with sectors heavily reliant on statutory obligations for public interest, promoting efficiency while maintaining legal integrity.

Transparency obligations in the context of automated decision making

Article 15(1)(h) of the GDPR determines that the data subject shall have the right to obtain information about "*the existence of automated decisions, including profiling, and, at least in such cases,* ***meaningful information about the logic applied and the significance and envisaged consequences of such processing for the data subject***".

On the other hand, Article 86 of the AI Act provides that natural person affected by a decision of a high-risk AI System "*which has an adverse effect on their health, safety or fundamental rights, shall have the right to obtain from the deployer* ***clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken***".

With regard to the information that the entity must provide to a data subject to comply with the GDPR, the recent judgment of the CJEU in C-203/22 analysed the information data subjects must receive in this regard and whether or not the algorithm underlying the automated decision must be provided to the data subject. The Court concluded that:

- The data controller must describe the procedure and principles applied in such a way that the data subject can understand which of his or her personal data have been used in the automated decision-making. The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the automated decision.

- GDPR requires the controller to provide **meaningful information about the logic involved in that decision, but '*not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm*'**.
- Regarding profiling, it may be sufficient to inform the data subject of the extent to which a variation in the personal data under consideration would have led to a different result.

Based on the decision of the Court, it may not be necessary to provide the detail of the underlying complex algorithm to comply with Article 86 AI Act, provided that alternative methods are found to provide a clear explanation to a natural person who should not be assumed to have the necessary knowledge to understand a complex algorithm. In order to avoid legal uncertainty, we **recommend that the EDPB and the AI Office, in the context of their forthcoming Guidelines on the interplay between the AI Act and the GDPR, align the transparency requirements set forth in Article 15 of the GDPR and Article 86 of the AI Act, in line with the decision of the CJEU**.

C. Co-existence of DPAs and other competent Authorities

There is a risk that divergent interpretations of the interplay between the GDPR and the AI Act by national supervisory authorities could lead to fragmented implementation across the EU. Based on the application of the AI Act, each Member State is in principle free to mandate the enforcement of the AI Act either to the national DPA or another competent authority. It is therefore necessary to promote coordination between data protection authorities and these new authorities to align criteria on key issues.

For more information:
Alexandra Maniati
Senior Director, Innovation & Cybersecurity
a.maniati@ebf.eu

Rachele Ceraulo
Policy Adviser - Data & Innovation
r.ceraulo@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 33 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.