6 June 2025

EBF_046788

EBF response to the European Data Protection Board's consultation on the draft Guidelines 2/2025 on processing of personal data through blockchain technologies

Key points:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's (EDPB) consultation on the draft Guidelines on processing of personal data through blockchain technologies.
- Three main points remain of fundamental priority throughout this response: first, the necessity to reaffirm the principle of technological neutrality by avoiding blanket disincentives against public blockchains; second, the acknowledgement that GDPR compliance is achievable on public blockchains using techniques like off-chain storage, pseudonymization, and zero-knowledge proofs and, third, the need for encouragement of risk-based, case-by-case assessment of blockchain architecture based on actual use cases and available safeguards.

General Remarks

We welcome the intention of the EDPB to clarify aspects regarding blockchain technologies, particularly the use thereof for personal data processing as required by the GDPR, and in light of the risks to the rights and freedoms of data subjects.

While specific comments on specific sections are provided below, we would like to highlight the following key points.

➢ Consistency with other pieces of legislation and cooperation with relevant supervisory authorities

As regards the banking sector, we strongly encourage the EDPB to **seek the opinion of European supervisory authorities on these draft guidelines** (e.g., ECB, EBA, ESMA) in the context of financial blockchains and digital assets. Indeed, many use cases may be at stake (cross-border payments, KYC, CBDC…) and a **close cooperation between all stakeholders** is essential. Indeed, it is of utmost importance to **consider GDPR compliance alongside compliance with other applicable EU legislations** (banking regulations, AMLR, MiCAR) to ensure plain consistency and applicability.

If published as they stand, we fear that the guidelines may **result in creating additional difficulties** for the use of blockchain in the EU. Instead, the EDPB could support EU innovation, for example by defining a concept of privacy-proofed blockchain in cooperation with relevant stakeholders, thus facilitating GDPR compliance of all parties involved.

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

- **Roles and Responsibilities of blockchain participants (Section 3.3)**

We would highly appreciate it if the EDPB could **further clarify the role and responsibilities of blockchain participants involved in the processing of personal data**. In particular, Section 3.3 should be further developed to provide more concrete guidance, considering that many blockchain participants are currently missing in the guidelines, notably miners, nodes, and networks.

We note that a similar exercise has already been carried out by some national DPAs: for instance, in its 2018 Analysis and Recommendations[1], **the French CNIL attempted to qualify the parties to a blockchain transaction under the GDPR**: accessors, participants, miners. We regret that the EDPB only gives some limited information to assess the qualifications of these parties and does not provide comprehensive guidance on the matter.

We would also like to note that any guidance on the parties involved in a blockchain environment (provider, consortium, miners, nodes, etc. should acknowledge that **the roles of these parties may vary depending on the type of blockchain in scope** (public, private, permission). However, as a general rule, **these roles should be clarified due to their consistency/recurrence across similar types of blockchains.**

In its Guidelines, the EDPB could be more prescriptive when it comes to the roles of the parties on a blockchain, similar to what previously done in its Guidelines 8/2020 on the targeting of social media users[2]. This would avoid potential inconsistencies between the roles assigned by the different participants in similar types of blockchain.

Finally, we note that, while the Guidelines reiterate the need to rigorously apply the definitions of "controller" and "processor", also in line with the EDPB Guidelines 07/2020,[3] they do not provide sufficiently detailed operational criteria to assign these roles in blockchain networks — especially in public and permissionless systems; this lack of clarity may thus create legal uncertainty for blockchain actors.

- **Lawfulness of the Processing (Section 4.4)**

The Guidelines briefly address the **importance of evaluating the lawful basis** for processing personal data under the GDPR. As a starting point, we would like to point out that, as referred to in **Paragraph 95** of the Guidelines, blockchains are only a technology (such as cloud computing or peer-to-peer networks), and cannot as such automatically constitute data processing. The blockchain technology itself does not perform the data processing; it is the applications running on the blockchain that handle the processing.

Having established that blockchains do not constitute data processing as such, we consider that only limited guidance is given on how to apply these principles. This clashes with the fact that a variety of lawful bases may be at stake, such as legal obligations, contractual necessity, and legitimate interests. We would **welcome more insights from the EDPB with examples/use cases to illustrate the choice of the legal basis**.

Section 1: Introduction

In **Paragraph 6**, the Guidelines state that the ability of blockchain technologies to offer strong technical guarantees in terms of integrity and availability via the cryptographic tools used is only a "*general assumption*". The reasoning provided is that "*there may not be standardised or formal agreements on the level or quality of the service provided*". While

we agree that in practice there may not be standardised or formal agreements in place, this does not mean that integrity and availability cannot be assured.

Blockchain technology is decentralized by design, but this does not preclude the existence of formal mechanisms to define, assess and monitor the quality of, broadly understood, the service provided. Even with public blockchain ecosystems, various tools enable an objective assessment of network health. Therefore, while traditional SLAs may be less prevalent (and restricted to centralized actors providing specific services, such as validation), such assessment and monitoring can ensure acceptable levels of integrity and availability. This is expected to evolve and mature over time, and we anticipate that standards will be further developed, implemented and enforced, also through usage and participation of regulated financial institutions in the governance and development of blockchain technology. **We therefore recommend that the EDPB reviews its statement in this direction**.

Section 3: Description of the Technology of Blockchains

3.1 Different Types of Blockchains

Paragraph 21 of the Guidelines provides examples of public permissionless blockchains (e.g., Bitcoin and Ethereum) but does not mention any private permissioned ones. For the sake of completeness, the EDPB could consider including examples such as Corda R3 or Quorum.

In **Paragraph 21**, blockchain technologies are defined as including *"transactions where the **identities** of the parties involved are visible to all"*. We note that, from a technical point of view, the term **"*identities*" is not appropriate and should be replaced with "public *addresses*" or "*pseudonymous identifiers* that are cryptographically derived**. It is also important to underline that, even though the address is visible, it does not reveal the identity of the parties involved (one doesn't know who effectively stands by the address). And it is a mere cryptographic derivation of the private key (public-private key pair) that is not publicly accessible.

3.2 Data inside a Blockchain

Paragraph 26 states that *"Each user participating in a transaction may, for instance, be associated with an identifier comprised of a **series of alphanumeric characters which looks random, and which constitutes a public key derived from a private key known to the users**. If the user is a natural person and those public keys can be used to identify the individuals by means reasonably likely to be used, for example in case of a **data breach**, then those identifiers qualify as personal data."* This brings up the following considerations:

- Given the nature of public keys, which are uniquely derived from a private key, we recommend that public keys are considered, at a minimum, as pseudonymised data.
- However, if there is no other data available to reasonably allow a third party to re-identify a data subject in a meaningful way, then this data should not be considered personal. In addition, a transaction log only containing an account number and transaction ID should not be considered as personal data, for it would not mean anything to anyone outside the organization involved in the transaction.

- Within the context of data breaches, the EDPB should expand on the possible malicious use of public keys. Also, the risk for the data subjects in the context of a data breach should be assessed based on the further use of the data.

Under **Paragraph 30**, the EDPB emphasizes that "o*n-chain data (including on-chain personal data) is not limited to the transaction data; rather, it may include other data structures stored on the chain, and that these data structures may also contain personal data*". In this regard, we note that possible solutions can be found to ensure compliance with the data minimization principle: for instance, requiring that the personal data stored on-chain is the minimum required data for processing to ensure that the blockchain technology is operational and secure.

Additionally, in **Paragraph 31**, the EDPB mentions that "*different approaches may be used to mitigate the data protection compliance risks associated with on-chain storage or to allow data subjects to exercise their rights*". We would welcome the inclusion of some additional examples or practical guidance on identifiers of the user, as the follow-on paragraphs only deal with data not strictly necessary to be "on-chain".

Paragraphs 32 and 33 illustrate various security measures/approaches that may be used to mitigate data protection compliance risks associated with on-chain storage. With regards to encryption algorithms, we believe it is important to bear in mind that, where encryption is broken, the data may be available on the blockchain without any time limit. Additionally, it would be worth mentioning other Privacy-Enhancing Technologies (PETs) that can be applied, such as multiparty computation, homomorphic encryption (or only minor references to ZK-proofs).

3.3 Roles and responsibilities

In the context of decentralised governance for blockchain, **Paragraph 36** of the Guidelines states that "*there must be a careful assessment of the roles and responsibilities"*. In this regard, while many of the actors operating on and developing blockchains are identifiable, with clear roles and responsibilities, we highlight that the **decentralised nature of blockchain technologies further complicates the identification of a clearly defined data controller(s)**, especially in relation to permissionless blockchains.

Under **Paragraph 40**, the EDPB considers *that "organisations should only explore different blockchain governance alternatives if well-justified and documented reasons hinder this preference. Where such reasons exist, organisations should also consider whether it is actually appropriate to use blockchain technologies at all."* **This approach seems at odds with the current broader work programme of the new European Commission to assess whether the current EU legislative framework** (e.g. CSDR, Settlement Finality Directive, Financial Collateral Directive) **is acting as a barrier to the development of DLTs** (acknowledging that existing rules were developed before the DLT was fully understood). Similarly, the present **Guidelines should not act to constrain firms' use of blockchains, nor suggest that emerging technologies should not be used altogether**.

In **Paragraphs 41 and 42**, when discussing the role of blockchain participants, we note that the Guidelines solely focus on nodes. We are of the view that all blockchain participants should be considered broadly, as opposed to nodes only, acknowledging that central entities are involved in operation and development of such blockchains.

In **Paragraph 42**, the EDPB states that in some circumstances, "*nodes would not determine the purposes and means of the processing itself and therefore might not be considered as controllers*". This raises the question of whether, in some cases, nodes might assume the role of controllers. However, **qualifying nodes as controllers raises considerable complications**. Among these, we would like to highlight the following considerations:

a. The precise number, location and identity of nodes on a blockchain can't be determined, given that they are spread over the globe;

b. Nodes only see the encrypted or hashed version of the data being inputted to the blockchain and thus are not capable of making any changes thereto, let alone of making decisions on the purpose and means of the data processing.

Additionally, in **Paragraph 42**, the EDPB states that *"processors process personal data on behalf of a controller and need to comply with Article 28 GDPR, otherwise they would act as controllers*". However, in the case of permissionless blockchains, this is not possible, as there is no control over their access.

Under **Paragraph 43**, the Guidelines mention that *"there may be cases where nodes should be qualified as controllers or joint controllers when nodes would exercise a decisive influence on the determination of purposes and essential means of the processing activity*". We submit that "***joint controller***" cannot be the correct term here as each node acts independently, as confirmed by the wording "*nodes may either individually exercise a decisive influence on the subset of transactions to be added to the next block they mine, or as a group by jointly agreeing (or not) on modifications of the protocols and the rules to apply".* Currently, **the Guidelines appear to confuse the concept of "jointly agreeing function" with "joint controller status"**.

Moreover, we stress that **it is unfeasible to agree on and apply Article 26 GDPR requirements to permissionless blockchains**. This is due to the fact that in permissionless blockchain there is no clear or central control over processing operations and decisions, as well as multiple "nodes", which entails a high difficulty in negotiating and agreeing upon a shared controller arrangement which would remain stable and enforceable over time across. In fact, the data is often processed for the joint purpose of a blockchain by several parties ("nodes"), who may not know each other. If you have 100+ nodes all processing the data, it's not realistic for them to co-ordinate with each other on Art 26 GDPR requirements, which requires the joint controllers to agree on who has to deal with data subject rights. The only way this works is if they each act as independent controllers and are responsible for their own processing.

Under **Paragraph 44**, the EDPB discusses instances of public and private permissionless blockchains in which nodes do not take instructions from any controller. For such cases, "*the EDPB strongly encourages the establishment of a consortium or any other type of legal entities among nodes*." We note that, from a practical standpoint, this is not always possible as the nodes do not follow an 'onboarding' process. Moreover, such a requirement is not realistic for already established permissionless blockchains, as:

- it would be contrary to the decentralized design of public permissionless blockchains which promotes security;
- public blockchains currently constitute a consolidated market standard, which our sector cannot ignore for the development of activities related to digital assets.

Section 4: Evaluating Blockchain-based Processing

4.1 Introduction

In this section, the Guidelines discuss the need for controllers to carry out a proper evaluation for their own processing before implementing a blockchain so as to ensure that the deployment of the technology is compliant with data protection principles. A list of questions to be answered as part of this evaluation process is provided under **Paragraph 46** "**necessity**", more specifically, the EDPB asks "*why is a blockchain necessary for this processing? What is the rationale for this choice? What are the alternatives?".* We argue that consumer choice may be considered as a factor in this regard.

4.2 Processing of personal data

In relation to the restrictions on public blockchains as per **Paragraph 49**, we are of the opinion that suggesting that public blockchains "*should only be employed if public access is necessary*" is unfairly restricting the use of blockchains. Consequently, **such a restriction results in a higher standard than the one imposed on other technologies and effectively goes against the principle of technological neutrality**.

Looking at the implications stemming from the storing of personal data on a blockchain, the following excerpt under **Paragraph 50** - *"technical impossibility cannot be invoked to justify non-compliance with GDPR requirements. Nevertheless, a proactive approach, combining organisational measures, techniques and governance models could transform perceived constraints into opportunities for compliance"* - raises the following considerations:

- With regards to the first sentence ("t*echnical impossibility*"), we are of the view that, as it currently stands, the Guidelines go as far as prohibiting an individual from choosing how to transact and make investments. More specifically, by claiming that technical impossibility is not a justification for non-compliance, the Guidelines effectively restrict consumer choice.
- **Footnote 17** makes reference to the Report of the work undertaken by the ChatGPT Taskforce; we note that these are very different technologies – ChatGPT, for example, does not require any identifiers – and should be treated as such.
- Finally, on the last sentence, we would appreciate it if the EDPB could expand on this holistic approach with practical possible examples.

Paragraph 52, which outlines the storing of personal data through data hashing, sparks the following reflections:

- The Guidelines remain open about what is meant by "salted hash" and throughout the draft, the term "salting" is never defined. There are a series of techniques which help to meet data subject rights requests, particularly by using multilayered blockchains or hashing out. It would be helpful if the EDPB could expand on some cutting-edge techniques focusing on "hashing out".
- The Guidelines also state that *"the hash will also be considered personal data*". We would like to recall that **hashes of data are irreversible**. It is therefore not clear why the EDPB concludes that hashes will be considered personal data when hashes are put on the blockchain. On this point, Recital 26 GDPR should remain the

standard for "identifiability", as confirmed in the Judgment of the General Court (Eighth Chamber, Extended Composition) of 26 April 2023 (Case T-557/20)[4]. It would be overly broad and counterproductive to a priori consider hash as personal data.

- Finally, the EDPB considers that *"after deletion of the secret key or salt, the hash should not be linkable to the original data, provided that the algorithm has not been broken, the keys have not been compromised or leaked, and the salt was not leaked or poorly chosen*". We would kindly request the EDPB to clarify whether, in that case, the hash could be considered as anonymised data, as it is not clear from the current drafting.

Under **Paragraph 53**, regarding cryptographic commitments, the Guidelines refer to a *"perfectly hiding state-of-the art scheme"*. We ask the EDPB to further elaborate on this reference.

In **Paragraph 54**, the EDPB considers that *"it is better to store the data in a form which is primarily intended to function as a proof of existence".* We call on the EDPB to confirm that the *"proof of existence"* is only a mere marker and therefore not considered as personal data.

In **Paragraph 55**, the Guidelines should provide more clarity on when the lifetime of the blockchain can be accepted as the data retention period with supporting examples.

Under **Paragraph 56**, the EDPB states that the *"measures presented above can be helpful for reducing risks to the data subjects […] they will also need to be accompanied by **other appropriate technical and organisational measures***". We would appreciate it if the EDPB could provide examples of other appropriate technical and organisational measures. Otherwise, we recommend deleting this sentence.

4.3 Principles of Data Protection

In relation to the fairness principle, as laid out in **Paragraph 58**, the Guidelines consider that the *"fairness principle requires that personal data should not be processes in a way that is unjustifiably detrimental, unlawful, discriminatory, unexpected or misleading to the data subject*". However, the principle of fairness should also entail that individuals have a choice as to what they do with their data.

The Guidelines address the data minimisation principle in **Paragraph 61**. On this point, we note the following:

- With regards to the architecture of blockchains, we are of the view that identifiers remain *"always visible, as they are essential for [the blockchain's] proper functioning. The CNIL therefore considers that this data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence*", as confirmed by the French CNIL in 2018.[5]

- The storing personal data in an off-chain database and hashing it onto the ledger respects the data minimisation principle (and the right to erasure, which is addressed under Section 5.2 of the Guidelines). This is because, once the off-chain data is deleted (when not needed any more), the on-chain hash becomes a random string of data without any meaning, as the on-chain hash has nothing to relate to.

This process thus ensures compliance with the minimisation principle, as well as the right to erasure.

Paragraph 63 concerns conformity of data processing by blockchain technology with the principle of storage limitation. The Guidelines state that *"Data deletion at the individual level in a blockchain can be challenging and requires ad-hoc engineered architectures. When deletion at the individual level has not been taken into account by design, this may require deleting the whole blockchain"*.

We recommend these two sentences to be deleted, as deleting the blockchain in its entirety is not realistically feasible, due to the following considerations:

1. There are backups for nodes;
2. The consortium needs to agree to delete the blockchain, which is unlikely to happen;
3. When it's a public blockchain, it is simply impossible;
4. The deletion misunderstands the fundamental structure of such technology, as no operator has unilateral control over public networks.

We suggest evaluating the possible impacts of **Paragraph 64** with respect to the AML regulation. The impossibility to link back an existing transaction "*involving a particular data subject with a future transaction involving that same person*" could prove problematic when banks need to fulfill their AML obligations.

4.4 Lawfulness of the Processing

The Guidelines briefly address the importance of evaluating the lawful basis for processing personal data under the GDPR. There is only limited guidance on how to apply these principles, where a variety of lawful bases may be in play, such as legal obligations, contractual necessity, and legitimate interests. **We would welcome more insights from the EDPB with examples/use cases to illustrate the choice of the legal basis**.

Under **Paragraph 71**, the Guidelines assess the role of consent as a legal basis for processing, as well as the conditions for consent to be considered valid. In particular, they state that "*where the storing of personal data is justified on the basis of consent, the personal data must be deleted or rendered anonymous if that consent is withdrawn"*. We suggest the use of "performance of a contract", as defined in Article 6(1)(b) GDPR, may provide a more suitable, alternative legal basis to consent, as it includes the consideration of the willingness of the user to transact.

4.5 International transfers

We are of the view that the EDPB adopts a broad interpretation of the concept of international data transfer in the blockchain context. In particular, it considers that a transfer may occur simply because data are accessible from nodes located outside the European Economic Area. This implies that the mere participation of validators, miners or other nodes based in third countries could trigger the application of Chapter V GDPR, requiring the implementation of appropriate safeguards — such as adequacy decisions, standard contractual clauses or binding corporate rules — without any specific exceptions for decentralised technologies.

We also note that the draft Guidelines appear to merely refer to the provisions of the GDPR and existing Guidelines and Recommendations. **We call on the EDPB to reconsider its approach and provide guidance in light of the particular specificities of blockchain technologies**. For example, the decentralised nature of the blockchain makes it very difficult for Data Exporters to perform the mapping of transfers and to maintain such mapping in the context of public blockchain.

If the recommendation of the EDPB is to map the physical localisation of every node and sign SCCs with them, this approach seems unfeasible, especially in the context of onward transfers and the interconnection of blockchains. For instance, in the context of the provision of cross border payment services through blockchains, this would bring back the same constraints and issues as with the correspondent banking network today. This approach is also restricted by the fact that new nodes can be added to the network by any actor having the necessary equipment and resources, leading to a dynamic validator network that is subject to change at any given time. We also note that blockchain technology often leads to data transfers outside of the EEA, especially when nodes located in third countries participate in the network. In public blockchains, these nodes are neither selected nor governed, creating significant challenges in terms of visibility, and consequently compliance.

The present Guidelines also present an opportunity for the EDPB to discuss the potential exemptions under Chapter 49 of the GDPR – for instance, exploring the applicability of Article 49(1)(g) on the register exemption.

In **Paragraph 74**, the Guidelines provide that "*these nodes are neither chosen or vetted, such as in public blockchains which may raise compliance concerns. Nevertheless, any transfer of personal data outside of the EU has to comply with the provisions of Chapter V GDPR".* This raises the following considerations:

- that consent under Article 49(1)(a) GDPR should be available for use in these matters;
- that the application of hashing and encryption techniques should be considered as appropriate additional technical measures as indicated under the EDPB Recommendations 1/2020.[6]

4.7 Data Retention Period

Under **Paragraph 78**, the EDPB states that *"[…] this is not a reason to assume that the lifetime of the blockchain is an appropriate data retention period"*. We would welcome it if the EDPB could justify its position. Given that the security of the technology lays in its auditability, it would be helpful if guidance could be provided in relation to what would be an acceptable timeframe which does not diminish the technology's security.

4.9 Data Protection Impact Assessment

In **Paragraph 92**, the Guidelines state that *"the controller always has the option to instead use a different model of blockchain or another technology that reduces, or does not introduce, such risks [to the rights and freedoms of individuals]"*. We are of the opinion that **this consideration is highly theoretical and not correlated to market practices**. On the topic of risks to the rights and freedoms of individuals, we would also welcome it if the EDPB could provide its view on the privacy risks related to blockchains.

Under **Paragraph 97**, in relation to the exercise of data subject's rights, **practical examples should be provided of how to effectively implement the rights of erasure, rectification, and objection** on immutable ledgers, particularly where encryption or commitment schemes are used. The guidelines emphasize compliance "*by design*," but don't provide realistic, technical blueprints or thresholds for when anonymization is "*effective*." The reference to "*innovative measures*" should also be expanded and supported by examples.

The EDPB concludes that the use of blockchain technologies will, in most cases, require a DPIA. This is based on the potentially intrusive nature of the processing, the possible involvement of special categories of data, and the limited control data subjects may have over their data. Although this is not a new legal obligation, the factors identified in **Paragraph 98** make it de facto mandatory to conduct a DPIA before deploying any blockchain project involving personal data. We also consider that the EDPB **requires the provision of a lot of information that goes beyond the letter of the GDPR**.

Additionally, **Paragraph 98** is problematic as it requires the assessment of the necessity of the use of blockchain, especially by considering it vis-a-vis other technologies. This seems to **clash with the technology-neutral approach behind the GDPR**, specifically Article 25, Article 32 and Recital 15, which does not bind compliance to specific technologies, leaving controllers free to choose the technologies they deem fit for the needed purpose.

Section 5: Data Subject Rights

5.2 Right to erasure and right to object

Within the context of the right to erasure and the right to object, under **Paragraph 102**, we note that the immutability of blockchain entries make it inherently difficult, if not impossible, to ensure the effective exercise of these rights.

It is further stated in **Paragraph 103**, in relation to the right to erasure and right to object, that the *"Controllers should consider this requirement early in the design phase and make sure that any personal data stored on the blockchain can be effectively rendered anonymous if an erasure request or objection is received".* We would **welcome practical examples to illustrate this recommendation**.

Additionally, *"the EDPB recommends looking at other tools if the strong integrity property of blockchains is not needed".* It is unclear which type of recommended technologies could be included. Examples like off-chain storage, hash, tokenization, could be provided.

Finally, in **Paragraph 104**, regarding the right of data subjects to have their personal data rectified or erased when clear text, encrypted or hashed data is recorded on a blockchain, the Guidelines state that "*personal data in those forms should be stored off-chain*". Does the EDPB consider "*off-chain"* storage as the only viable solution in the above-mentioned cases?

III. Annex A – Recommendations

In general, we note that the feasibility of **Recommendations 4, 5, 9, 11 and 16** are questionable. More specifically, they seem to imply that, if in a given situation, due to the nature of the blockchain, it is impossible to block certain data, then the blockchain is by definition in contravention of the GDPR.

For example, **Recommendation 5** on "Trust", which states that "*the choices of implementation should include mechanisms for assuring trust including in software and nodes' identities*", raises the question of how this can be put into practice for permissionless blockchains.

For more information:
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 32 national banking associations in Europe that together represent a significantmajority 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. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. 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