20 November 2024

EBF_046647

EBF response to the European Data Protection Board's consultation on the draft Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

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 based on Article 6(1)(f) GDPR, hereinafter – the Guidelines.
- We welcome that the EDPB Guidelines recognise legitimate interest – as a legal basis for processing personal data – on an equal footing with the other five legal bases of Article 6 GDPR, without any hierarchy between them. However, the **EDPB must ensure that these Guidelines do not diminish the equal footing of legitimate interest by including too restrictive provisions for their use**.
- **The EDPB should seek to provide additional clarity to the applicability of Article 6(1)(f) GDPR, thus ensuring that the Guidelines are simple, concise, and clear** with reference to practical examples. However, in several sections, the provisions appear to extend the obligations of the GDPR, by creating for example new obligations, new concepts or new categories of personal data.

General Remarks

We welcome the intention of the EDPB to clarify aspects regarding Article 6(1)(f) GDPR and whether it may be invoked as a valid legal basis for the processing of personal data.

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

➢ Distinguishing between legal bases

Our sector is strictly regulated by law. This means that different grounds can apply to the processing of personal data. In this regard it would be useful if the EDPB could provide, as a helping hand, **principles or illustrative parameters to help distinguish between the applicability of Article 6(1)(c) and Article 6(1)(f) GDPR**. These could be used at the discretion of the data controller, bound to the **accountability principle**, and given the **risk-based nature of the GDPR**. For example, the controller may rely on a legal obligation as a legal basis of processing when non-compliance with the law would result in an administrative penalty even if the law is not sufficiently clear; and also, when processing is supported by guidelines and opinions of the regulators.

➢ The status of WP29 Opinion 06/2014 on the notion of legitimate interests of data controllers

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

We would also highly appreciate if the EDPB could **clarify the status of WP29 Opinion 06/2014 on the notion of legitimate interests of the data controllers** under Article 7 of Directive 95/46/EC. Given that in the Guidelines the EDPB has not provided a new guidance on some aspects analysed in the mentioned Opinion, it would be important to clarify whether this Opinion can still be applicable.

- **Lack of practical examples**

We would also appreciate **examples of processing personal data in contexts other than those already illustrated in the Guidelines, such as for the use of artificial intelligence**. Using personal data for AI training and testing purposes is of utmost importance, especially when algorithms or AI systems need to be used for fraud prevention or transaction monitoring as per the AML legislation. Not being able to train and test algorithms would lead to high risks, since the accuracy of such algorithms could not be granted. Legitimate interest must be possible for this type of processing and should therefore be provided for by the EDPB.

- **Compliance with the boundaries of the GDPR**

In several sections, the EDPB appears to add to and extend the obligations of the GDPR, by creating, for example new obligations, new concepts or new categories of personal data. For instance, the EDPB equates sensitive data to special categories of data. This interpretation, however, has the effect of over-broadening the definition of sensitive data. We therefore recommend that the Guidelines do not add to the GDPR and its provisions.

I. Introduction

In **Paragraph 7**, reference is made to the **CJEU judgment *Rīgas satiksme*** to imply that the "*"balancing exercise" between the fundamental rights, freedoms and interests at stake must be performed for each processing to be based on legitimate interest as a legal basis*". It should be noted that this implication does not follow from paragraph 28 of such judgment.

Indeed, paragraph 28 reads as follows: "*In that regard, Article 7(f) of Directive 95/46 lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence*."

There is no mentioning nor reference to the "balancing exercise" being carried out for each processing activity. A financial institution may carry out different types of data processing, many of them relating to the same legitimate interest. In order to help compliance, we would appreciate it if the EDPB could **allow clustering similar data processing that, due to their close similarity, could be brought under one legitimate interest for which one balance exercise can be performed**.

II. Section 2: Elements to be taken into account when assessing the applicability of Article 6(1)(f) GDPR as a legal basis

It is stated in **Paragraph 12** that "*The [legitimate interest] assessment should be made at the outset of the processing, with the involvement of the Data Protection Officer (DPO) (if designated)*", with a reference to Article 38(1) GDPR.

Although according to Article 38(1) GDPR, the DPO shall be involved by the controller and the processor in "*all issues which relate to the protection of personal data*", under Article 39(2) GDPR the DPO "*shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing*".

We would like to recall that, in its Guidelines on Data Protection Officers, the WP29 clarified that the risk-based approach "***requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks***" (para 4.4). With due regard to the enormous workload of DPOs in the financial sector, we believe that **the controller and the processor can specify in internal procedures when the involvement of the DPO is mandatory, e.g. when the processing is likely to result in a high risk to the rights and freedoms of data subjects**. In the event the processing would result in no or lower risks, the involvement of other specialists in data protection can be ensured. Therefore, **we strongly recommend that the present Guidelines refer to the risk-based approach** under the above-mentioned WP29 Guidelines. For example, it would be preferrable to see the involvement of the DPO in the balancing test of individual processing activities that related to the performance of a Data Protection Impact Assessment (DPIA).

In **Paragraph 12**, the following sentence should also be clarified: "*This assessment should follow the three-step process outlined below, although in some circumstances the examinations of the second and third conditions may merge in so far as the assessment of whether the legitimate interests pursued by the processing of personal data cannot reasonably be achieved by less intrusive means requires a balancing of the opposing rights and interests at issue*." While we welcome the practical approach of the EDPB (taken from the CJEU) when stating that the second and third steps of the three-step process can be merged, the condition the EDPB attaches to being able to merge these two steps is, however, not entirely clear. We recommend that the EDPB provides **examples of when such two steps can be combined**.

A. 1st step: Pursuit of a legitimate interest by the controller or by a third party

In our sector, there are examples of data processing that serve the data subject's interests more than the data controller's. For instance, we consider the processing of personal data to gain insights into the customer's financial situation for them to avoid getting into financial difficulties as a situation where the data processing is also beneficial for the data subject.

This may raise the question of whether the legitimate interest of the data subject could also constitute grounds for processing. It might help the readers of the Guidelines if reference is made to the definitions of "data controller" and "third party" in the GDPR. The data controller is not the data subject and data subjects are explicitly excluded from the definition of "third party". This leads to the conclusion that this article is meant for legitimate interests of the data controllers and third parties not being the data subject. Despite this clarity, the sector would appreciate that this is explained in the guidance.

It would be helpful to add that, **when data processing is beneficial for data subjects (that is, the processing serves the interests of the data subjects), the data controller may have a legitimate interest in catering for that benefit**. In this respect, the Guidelines could clarify that the interest of data subjects in a given data processing activity are taken into account when performing the three-step assessment,

particularly the third step. When the processing is done mainly for the benefit or interest of the data subject, it will be easier to argue that the processing that the data controller wishes to undertake does not override the interests of data subjects, because in fact it serves also the interests of the latter. This can help reach the conclusion that the processing can be based on this ground - provided that the other two steps are adequately substantiated.

2. Interest pursued by the controller or a third party

In **Paragraph 19**, the Guidelines state "... *the CJEU found that, even though the sharing of information with law enforcement agencies in order to prevent, detect and prosecute criminal offences is a legitimate interest as such, it is not capable, in principle, of constituting a legitimate interest pursued by a controller whose activity is essentially economic and commercial in nature, as it is unrelated to its economic and commercial activity*."

We would like to make the following considerations:

a. In principle, the sharing of information with law enforcement agencies to prevent, detect and prosecute crimes is generally based on the legal basis of the legal obligation as it is regulated by regulatory provisions and is therefore based on legal obligations (see e.g. anti-money laundering obligations). However, in cases where a controller carries out activities which do not fall within specific legal obligations set out in laws and regulations, the sharing of information could be based on legitimate interest and other legal grounds.

b. In addition, the fact that **the activity carried out by the data controller is a commercial activity cannot in itself limit the collaboration of the data controller with public parties**, and it should be clarified that such collaboration should not be considered as "unrelated to its economic and commercial activity"

It is also not clear in the context of banking operations when reference can be made to the legitimate interest of third parties in these cases. We recommend that the Guidelines further clarify the statement under Paragraph 19 with some examples.

For example, if it is prescribed that banks have to establish appropriate measures to detect and prevent certain illegal activities (without the details and specifications of such measures), the personal data processing activities may be appropriate measures which are not prescribed precisely, and if further clarification is not provided in the Guidelines, this may be interpreted as if banks could not rely on legitimate interest as a legal basis, nor compliance with a legal obligation. In this regard, further clarification concerning the interpretation of and the interplay between Article 6(1)(c) and (f) should be provided.

Under **Paragraph 20**, the EDPB states that "*the legitimate nature of the interest of a third party must be assessed following the same criteria which apply with respect to the controller's own interests*." We find this statement problematic: it cannot be reasonably expected from a data controller to be aware of the legitimate interests of a third party and carry out the assessment of the legitimate nature of the interest of the third party as thoroughly and following the same criteria for which it would consider for its own interests.

Paragraphs 21 to 25 illustrate some of the contexts where personal data may be processed in the interest of a third party. For example, under **Paragraph 25**, the EDPB mentions that the general public interest or the interest of a third party could constitute a

legitimate interest for the controller, subject to justification, for further processing. This seems to indicate that it is possible to justify the anti-fraud processing based on legitimate interest when such activities do not fall within such specific legal obligations set out in laws and regulations. While we welcome such clarification, we are of the opinion that the interpretation of the EDPB is overly restrictive. This creates an area of uncertainty while the Guidelines are there to guide. Further clarification is therefore needed (please refer to our remarks in **Paragraph 107**).

Finally, we recommend that the Guidelines consider additional contexts where personal data may be processed in the interest of a third party. This may include:

- Cases where **data is made available by a data controller to a third party where data (i) may facilitate compliance with a legal obligation incumbent on the data controller or (II) is used to improve a provider's technology.** For example, legitimate interest could be a valid legal basis to improve an algorithm deployed to analyse digital asset transactions carried out by a service provider in order to facilitate the monitoring and follow-up of these transactions as part of the "Know you transactions" process. This type of context, however, is not addressed in the Guidelines, while it raises questions in the context of the use of legitimate interest.
- Situations where clients that have been victims of fraud would need the name and address of the client to whom the money had been transferred to, so the victim can start legal proceedings.
- Cases where a client has made a money transfer to the wrong person by mistake. If this person denies reimbursement after the bank has asked them to return the money wrongfully transferred, that information can be disclosed to the person who made the mistake allowing them to recover its funds, for example through the courts.
- Banks - given the expertise they have in micro- and macroeconomics - may need to study client data for high-level analysis that often is published for statistics, research, general public interests, etc.

B. 2nd step: Analysis of the necessity of the processing to pursue the legitimate interests

Paragraphs 28 and 29 bring up several considerations:

- Whereas the sector acknowledges that the processing of personal data for this ground should be limited to what is strictly necessary, we are also of the opinion that **what is strictly necessary may vary depending on all facts and circumstances**. In order to meet the need for this guidance to be applied uniformly, we would suggest **adding the criterium "reasonably"**, which the EDPB already recognises in the Guidelines under Paragraph 29.
- **The criteria set out in paragraph 29 concerning the need to justify necessity by demonstrating that other less restrictive means could not be deployed to meet the legitimate interest could constitute a significant brake on innovation in certain cases.** There may be situations in which, despite the apparent intrusiveness of the method for data processing, such method is considered "adequate and relevant and limited to what is necessary", to put it in the terms of the Meta case. For example, methods to help identify the client for full online banking services, where there are no physical offices where clients can go identify themselves in front of an employee. There is a legal obligation on the sector

to identify our clients, but the method is left to the discretion of the banks. To the extent that it cannot be argued that the given processing does not fall under Article 6(1)(c), it would help the sector if the Guideline were to add that, in specific sectors, certain restrictive measures could be justified by specific circumstances, where the combination of legal requirements, innovation in providing services, and new threats would justify the data processing.

C. 3rd step: Methodology for the balancing exercise

The sector welcomes the description of what the EDPB understands as rights and freedoms that should be considered and what interests of the data subjects seem to be. However, the Guidelines do not describe how these rights need to be balanced against the legitimate interests of the data controllers. In general, we would highly appreciate a **more precise methodology for carrying out the legitimate interest assessment**, particularly when it comes to performing the **balancing test** and the various elements the controller must identify and describe (i.e., the data subjects' rights, freedoms, interests, its reasonable expectations) to be able to perform a meaningful assessment. However, we are of the view that only a formal description of data subjects' rights, freedoms, interests, and expectations does not contribute to proper balancing with the controller's legitimate interests. We are of the view that more practical guidance would be appropriate, resulting in shorter and to the point assessments that can be carried out more comfortably by someone without a legal training and without having to ponder ethical questions on the balancing of rights.

1. Data subjects' interests, fundamental rights and freedoms

Paragraph 37 states that "***The fundamental rights and freedoms of the data subjects*** *include the right to data protection and privacy, but also other fundamental rights and freedoms, such as the right to liberty and security, freedom of expression and information, freedom of thought, conscience and religion, freedom of assembly and association, prohibition of discrimination, the right of property, or the right to physical and mental integrity,* ***which may be affected by the processing, either directly or indirectly****."*

We strongly recommend that the Guidelines limit the reference to the direct impact on the rights and freedoms of the data subjects, as the reference to indirect impacts seems to be too indeterminate and extensive a concept. Direct impacts are already difficult to grasp, making indirect impacts almost impossible to consider.

Finally, **paragraph 38** notes that "*The interests of the data subjects to be taken into account as part of the balancing test include any interest that may be affected by the processing at stake, including, but not limited to, financial interests, social interests or* ***personal interests***." Given that "*personal interest"* is a vague and abstract term under the draft guidance, we recommend that the EDPB provides practical examples as to what could constitute a personal interest that controllers need to take into account when performing the balancing test. More generally, we would like to stress that, the clearer the examples and instructions provided by the EDPB, the more precise the assessments can be performed by controllers. Otherwise, the controller might not be aware of all dimensions of impact which the particular processing can cause to the data subject.

2. Impact of the processing on the data subject

On **paragraph 39**, the Guidelines state that "*This assessment should focus on the various ways in which individuals may be affected – positively or negatively, actually or* ***potentially*** *– by the processing of their personal data*." The reference to "potentially" seems too hypothetical and indeterminate. Therefore, we ask the EDPB to limit the scope of such an assessment to the actual impact of processing on data subjects. This does not seem to make the point that the interest in processing the data must be real and present and not speculative (see Paragraph 17, third indent). Alternatively, it should be clarified that what is expected from the controller is to make reasonable efforts to assess the potential impact of processing activities on data subjects. Finally, we ask the EDPB to clarify in the Guidelines whether "actual" impacts could also be reduced by taking mitigating steps, in order not to over-broaden the scope of the assessment.

2.1 The nature of the data to be processed

Paragraph 40 illustrates the elements that controllers need to pay attention to when qualifying the nature of data to be processed as part of the balancing exercise. We would like to highlight the following considerations:

- Special categories of data, as per Article 9 GDPR, are referred to and defined in the Guidelines as "sensitive data". The sector processes data that could be considered sensitive but without falling under the scope of the definition of special categories of data as per Article 9 GDPR. The text suggests that sensitive data are elevated to the status of "special categories of data", which from a legal perspective is inaccurate. We would suggest using, for example, "spcd" to refer to "special categories of data" rather than sensitive data.
- Under the first indent, the text states that "*It is irrelevant whether or not the information revealed by the processing operation in question is correct and whether the controller is acting with the aim of obtaining information that falls within one of the special categories referred to in that provision. Hence, according to the jurisprudence of the CJEU, the relevant question is whether it is objectively possible to infer sensitive information from the data processed, irrespective of any intention of actually doing so*." **We are of the view that this interpretation has the consequence of over-broadening the definition of sensitive data, adding to the GDPR.** With regards to the third indent, the EDPB mentions and seems to be creating a **new type of data which is qualified as being "more private". This category of data does not exist under the GDPR** and the EDPB is not empowered to create new categories of personal data adding to the GDPR by means of Guidelines. We are of the view that the concept of private data could be interpreted randomly, as here there is a reference to the subjective assessment made by the data subject and not to a normative definition. If the intention of the EDPB is to indicate that, in the case of data of public nature, the impacts of the processing are likely to be less significant, this should be clearly stated. It is **essential that all references in the present Guidelines align with GDPR concepts**.

Paragraph 41 states that "*As a general rule, the more sensitive or private the nature of the data to be processed, the more likely it is that the processing of such data will have a negative impact on the data subject*". We are of the opinion that this postulate by the EDPB prejudices the result of the balancing test. When carrying out a balancing test, it is necessary to take into account the benefit for the data subject (i.e., health, safety, etc.) and the reproaches that could be levelled at the data controller for not taking all the

necessary measures to preserve the interest of the data subject. What if there is a conflict between the interest of the data subject and his/her freedoms and rights? This could be the case when clients want their bank details to be protected from fraud, but this requires the bank to study their payment or other details in a way that the client might not expect.

2.2 The context of the processing

In the second and fifth indents of **Paragraph 43**, there are two examples that would require further elaboration. With regard to the context and methods of processing, reference is made to the relationship between the controller and the data subject. More specifically, a different assessment will be necessary if the data subject is an employee or when the data subject is a customer. It would help to include which circumstances mean that a different approach is needed. The same would apply to the example of vulnerable individuals: under what circumstances would the vulnerability of an individual preclude a controller from relying on legitimate interest? There might be situations in which the vulnerability of certain clients can be the reason to process data, for example when a bank would want to help certain vulnerable clients to use banking apps and understand the information provided.

We would also expect the following factors to be relevant in the context of processing and therefore mentioned in paragraph 43:

- Whether or not the processing has benefits for the data subject as well;
- The possibility for the customer to "opt out" from the processing (as mentioned in the WP29 Guidance on legitimate interest (pp. 43-44);
- The nature of the interest pursued by the controller; we believe it is relevant whether the controller is pursuing only its own commercial interest, whether there are broader societal interests involved, or whether the controller is processing data in order to comply with demands of its (financial) supervisors.

2.3 Further consequences of the processing

Paragraph 45 outlines the factors that data controllers may need to take into account as part of the balancing exercise when assessing any further consequences of the processing. **The consequence referred to in the first indent should be deleted. The data controller cannot be expected at all times to know what future decisions may be taken, nor can it be expected from a data controller to know what third parties may do with the data**, for example in the event of disclosure based on the legitimate interests of a third party to whom data may be disclosed. More generally, we are of the view that **factors listed in this paragraph are not easily declined in practice**. Therefore, it would be useful if concrete examples were formulated.

Paragraph 46 states that "*the controller may need to take into account also possible broader emotional impacts resulting from a data subject losing control over personal information, or realising that it has been misused or compromised*." The emotional impacts of data processing activities on a data subject are difficult to predict in practice and vary greatly depending on the data subjects and the context of the processing. Taking into account emotional impacts requires a very subjective evaluation and a case-by-case assessment according to the personality, psychology, feelings, and personal background of each individual at a given time (and what matters to one individual may not matter to another and vice versa). **It cannot be reasonably expected from the data controller to take into account the emotional impact of a given data processing**. This would also be in contradiction to Paragraph 47, where it is stated that controllers cannot consider

that all data subjects share the same interests. **We strongly recommend deleting this requirement.**

In addition, the meaning of this paragraph is not entirely clear; if it refers to online tracking activities aimed at the general public, it should be noted that this type of activity (e.g. profiling cookies) is usually based on the legal basis of consent. It would therefore be useful to have some possible examples referring to other types of treatment.

Under **Paragraph 47**, the EDPB writes that "*the controller should not base its assessment of the interests at stake on an assumption that all of the affected data subjects share the same interests when it has – or should have – concrete indications of the existence of particular individual interests or when, from an objective perspective, it is simply not likely that all data subjects will have the same interest(s) the controller has assumed*." In practice, however, these indications are difficult to implement in the context of the processing carried out by a bank, in which the balancing, in most cases, must necessarily take as a reference the characteristics generally referable to customers as a whole or to certain categories of subjects and not the characteristics of individuals to the exclusion of subjects belonging to clearly identifiable categories (e.g. minors, vulnerable subjects, etc.).

3. Reasonable expectations of the data subject

In the balancing exercise, one of the elements to take into account is the reasonable expectation of the data subject in relation to the proposed processing. In this regard, paragraph 52 states that "*The fact that certain types of personal data are commonly processed in a given sector does not necessarily mean that the data subject can reasonably expect such processing*." **We propose to delete or rather circumstantiate the sentence, given that it does not seem entirely coherent**. Indeed, the practices in use in certain sectors/contexts could in some cases play an important role in assessing the expectations of the data subjects. Moreover, the subjective view of a data subject that does not expect a bank, for example, to use data processors should not be seen as an impediment to base the disclosure of personal data to that processor. It would be convenient to clarify that subjective expectations of the data subjects do not fall under "reasonable expectations of the data subject".

We are also **concerned about Paragraph 53**, which states that "*the mere fulfilment of the information obligations set out in Articles 12, 13 and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing*." Such a conclusion is misleading and contrary to the citied Articles 12, 13 and 14. Information obligation and transparency requirement stipulated in the mentioned articles is imposed on the controllers with the exact aim of informing data subjects about the processing of the personal data so that the data subjects can "vindicate their rights and hold data controllers accountable for the processing of their personal data" (see WP29 Guidelines on transparency, para. 55). One of the key principles of the GDPR is transparency about data processing, with intelligible and easily accessible information; **it is precisely through this transparency that the reasonable expectations of the data subject are forged, even before determining the legal basis chosen for processing**.

Additionally, under **footnote 61**, the EDPB writes that "*it should be noted that contractual provisions regarding personal data may have a bearing on the reasonable expectations of data subjects*." We would like to point out that the GDPR mentions that contractual clauses contribute to this information, but in an additional way. We suggest the footnote be

included in the main text. The contextual information that contractual clauses provide help indeed in stating that the data subject could have expected the processing.

In Example 5 (after Paragraph 54), reference is made to product improvement. In that specific context, the EDPB, referring to the *Meta* case, states that in the context of a service that is free of charge, it cannot be reasonably expected for "*those data to be processed even for other purposes such as product improvement*".

At the end of this text, a footnote refers to paragraph 123 of the Meta case. This paragraph reads as follows: "*However, **subject to final assessment by the referring court** in that respect, it **appears doubtful** whether, as regards the data processing at issue in the main proceedings, the 'product improvement' objective, given the scale of that processing and its significant impact on the user, as well as the fact that **the user cannot reasonably expect those data to be processed by Meta Platforms Ireland**, may override the interests and fundamental rights of such a user, particularly in the case where that user is a child.*" The statement of the EDPB goes far beyond and does not faithfully reproduce what the court in fact is saying.

There may be situations in which the processing of data for product improvement is to be expected, provided that the data controller is transparent on it and applies the principles of necessity, data minimization, etc.

4. Finalising the balancing test

We would like to reiterate that more specific guidance should be provided on the exercise of balancing the interests. The enumeration of the interests and fundamental rights, ascertaining whether the data is sensitive or belongs to special categories of data, describing the context, enumerating further consequences for the data subject, ascertaining if the data subject could or could not expect the processing are just the ingredients that need to be weighed. **The guidance does not explain how this weighing exercise needs to be done. How can controllers get to the conclusion that they managed to strike the right balance?**

In **Paragraph 57**, whereas we understand that the data controller is already bound by certain obligations, such as transparency, it should be noted that the fact that those measures are already provided may help being able to argue that there is a legitimate interest. It goes too far to say that even when a controller complies with all the GDPR requirements, that this does not help in assessing whether there is a legitimate interest and that always mitigation measures need to go beyond what is already being done.

Paragraph 58 states that "*if controllers decide to implement mitigating measures, they should perform the balancing test anew, in order to assess whether the legitimate interest(s) being pursued are overridden by the data subject's interests, rights and freedoms, after the adoption of the mitigating measures*." **The repetition of the balancing process appears to be an unnecessary procedural burden**, given that the evaluations could all be made within the framework of a single balancing exercise. **We recommend that this paragraph be deleted.**

III. Section 3: Relationship between Article 6(1)(f) GDPR and data subject rights

2. Transparency and information to be provided to data subjects

Under Section 3 of the Guidelines, the EDPB outlines the relationship that exists between Article 6(1)(f) GDPR and a number of data subject rights under the GDPR. It is unclear why all these data subject rights are being looked at in the course of the Guidelines. This could imply that a data subject right (such as the right to the restriction of processing) might be looked at differently depending on the legal basis.

Under **paragraph 68**, the EDPB notes that "*the controller can also provide the data subject with information from the balancing test in advance of any collection of personal data*" and that "*information to the data subjects should make it clear that they can obtain information on the balancing test upon request*. However:

- **There is no obligation under the GDPR requiring controllers to disclose the legitimate interest assessment or parts of it to the data subjects**. **Nor does it provide for this right in favour of data subjects. Therefore, disclosure of such information should be made only at the discretion of the controllers.**
- In addition, assessments made by the controller may contain internal and confidential information not only about the economic activity of the controller but also internal methodology, processes, commercial strategy and other *know-how* elements which does not have to be communicated to the data subject.
- Moreover, this obligation raises practical difficulties because it would require updating the information for each processing operation that has been the subject of a balancing test and informing the people concerned in advance.

Paragraph 68 also states that "*the mere fulfilment of information duties according to Articles 12, 13 and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing*." Similar to our concerns under paragraph 53, such conclusion that even if the data subject is informed about the processing but still cannot expect the processing to take place is misleading and contrary to Articles 12, 13, and 14.

Based on the concerns articulated above, **we recommend that this paragraph be deleted**.

3. Right of access

The recommendation in **Paragraph 70 goes beyond what is stipulated in the GDPR**. The data subjects are already informed on the basis of Articles 13 and 14 of the GDPR on the grounds of processing. This is a repetition. **It should not imply a new obligation for the data controller. In any case, when a data subject exercises his or her right of access, it should be sufficient to refer to the information already available or provided in the privacy notices on the grounds of processing.**

4. Right to object

According to **paragraph 71** "*the fact that the data subject has not elaborated much on their "particular situation" in their objection is not per se sufficient to dismiss the objection*." It would seem appropriate to clarify that the interested party who claims the existence of a particular situation is still required to allege and prove the situation.

The last two sentences of **Paragraph 73** are problematic. Data controllers decide how their business and operational processes are designed, taking into account, among others, the principles of privacy by design and default. If a customer objects to how a given generic process that has been internally validated by the stakeholders within an organisation, including the DPO, objects to the processing that in that context is taking place, it should

be possible for the data controller to adduce business interests not to accept that objection. It should be added that business interest, including generic processes, can be sufficiently important, justifying not honoring an objection request of a single customer.

IV. Section 4: Contextual application of Article 6(1)(f) GDPR

1. Processing of children's personal data

Paragraph 95 addresses the processing of personal data of children. It mentions that "*Therefore, unless controllers can demonstrate that the activities in question which rely on the processing of children's personal data do not negatively affect the children's interests, such activities should not be undertaken*". It is not exactly clear what is meant with "such activities". We assume that these are the activities mentioned in the previous sentence – marketing, creating personality and user profiles, or offering services aimed directly at children – but we would like clarity on this point.

Paragraph 97 states that "*a child is every human below the age of majority*." Besides the fact that these ages might differ across EU member states, this statement is not in line with Article 8 GDPR, in which the age of 16 relating to the processing of personal data is mentioned.

3. Processing for the purpose of preventing fraud

We welcome **Paragraph 107** in that it recognises that fraud detection and prevention mechanisms may be required by law. Indeed, in our sector, fraud prevention goes beyond the concept of legitimate interest. It is an expectation from the legislator, the financial supervisory authorities, and the public in general.

The Payment Services Directive (PSD2), under Recital 95, makes direct reference to the risk of fraud:

> "*Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce.* ***All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud***."

The future Payment Services Regulation (PSR), in its Article 83(1)(c), contains the explicit obligation to take measures against fraud:

> "*Payment service providers shall have transaction monitoring mechanisms in place that: support the application of strong customer authentication in accordance with Article 85; exempt the application of strong customer authentication based on the criteria under Article 85(11), subject to specified and limited conditions based on the level of risk involved, the types and details of the data assessed by the payment service provider;* ***enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services***."

We would therefore appreciate it if the Guidelines could recognise that **for banks, it is not simply a matter of legitimate interest. Banks are not at liberty to discard implementing measures to prevent fraud**. Failure to implement such measures can result in sanctions for those banks. Of course, in addition to the compulsory aspect, banks also believe that it is necessary that such measures are in place not only to protect their

integrity and maintain trust in the sector, but also to protect their clients (both funds and data).

It should be noted that sectoral legislation leaves room for data controllers to develop and apply such measures. In this regard principles or illustrative parameters as referred to in the first section of our general remarks would help.

In relation to the reliance on legitimate interest for fraud detection/prevention, the Guidelines appear to adopt a somewhat limitative approach.

For example, under **paragraph 105**, the text states that "*Controllers should be specific about what type of fraud they are trying to prevent, and what data they really need to process in order to prevent that type of fraud. The fraud the controller is trying to prevent should be of substantial importance, otherwise, the balancing of interests will most likely turn out in favour of the data subject, and the controller will not be able to rely on Article 6(1)(f) GDPR in this respect*."

It seems **unlikely that any type of fraud prevention would not be 'of substantial importance' and therefore firms, including banks, would likely always have a strong legitimate interest in carrying out processing for the prevention of fraud**. In addition, it must be considered that the tools and methods with which fraud is implemented are constantly evolving and increasingly sophisticated. It follows that effective fraud prevention cannot be subject to excessively strict limitations. It should also be taken into account that in the banking system, fraud prevention is usually mainly implemented in the interest of the customers themselves, (e.g., to ensure the security of their financial and personal information, and to help customers avoid falling victim of fraud), but also more broadly, to ensure the stability and integrity of the financial sector, and maintain society's trust in the sector.

Paragraph 106 states that *"a generic reference to the purpose of "combating fraud" to define the legitimate interest, for example in the privacy policy, is not sufficient to meet the transparency and documentation obligations under the GDPR*." We would welcome a clarification from the EDPB on its expectations in terms of transparency and documentation obligations under the GDPR. If there is too much information available for the public, the risk exists that fraudsters learn how to circumvent preventative measures (gaming the system).

4. Processing for direct marketing purposes

4.1 The notion of direct marketing

Paragraph 109 states that "*[…] In particular, the CJEU found that to assess whether a communication is made for direct marketing purposes it must be ascertained whether such a communication pursues a commercial purpose and is addressed directly and individually to a consumer […]*". In a scenario where a commercial communication is made to a company, but is sent to the e-mail of an employee of that company (e.g. employeefullname@companyname), can legitimate interest be considered as an appropriate legal basis? Clarity on this aspect would be helpful.

4.2 Compliance with specific legal requirements that preclude reliance on Article 6(1)(f)

Paragraph 113 mentions that "*Before engaging in the processing of personal data for direct marketing purposes, controllers should consider specific European, as well as*

national, legislation which may require consent for certain operations in the context of direct marketing, or prohibit some kinds of direct marketing". In the paragraphs that follow, it seems that the EDPB is of the opinion that the processing of data directly relates to the way the message will be sent. These require two separate legal considerations.

4.3 *Case-by-case assessment to be made when reliance on Article 6(1)(f) is not precluded by law*

We would like to raise the following considerations related to **paragraph 120**:

- "*For example, the balancing test would hardly yield postive results for intrusive profiling and tracking practices for marketing purposes, for example those that involve tracking individuals across multiple websites, locations, devices or services*." This example is not clear in the context of these Guidelines. The processing based on tracking (profiling cookies, etc.) should be based on the legal basis of consent not on legitimate interest.
- The EDPB also argues that legitimate interest is not compatible with processing to send personalised advertising, while it can be relied upon when sending the same commercial communication to all existing customers who have already bought similar products. We view this position as very restrictive, especially after the decision in CJEU in the KNLTB case. Provided that the three-step test is adequately effected, adequate measures are in place to preserve the fundamental rights and freedoms of individuals and their interests are also taken into account, personalised advertising should be capable of being based on legitimate interest.

5. Processing for internal administrative purposes within a group of undertakings

On data sharing within a group of companies: we do not understand why data sharing could only be done between companies that would necessarily be controllers (see Paragraph 123).

We would also welcome further clarification and examples on data sharing for administrative purposes for both customers and employees, going beyond the processing of personal data for statistical purposes. One example is not sufficient. Specifically, we recommend that the EDPB considers the following examples:

- **Processing of judicial data for the purpose of assessing the reliability of partners and suppliers**: it would be desirable for the EDPB to recognise a legitimate interest worthy of protection in the case of processing of judicial data relating to subjects not falling within the category of customers (of duration and/or occasional) pursuant to anti-money laundering legislation, which is aimed at verifying in advance the reliability of the counterparties (even in the case of sponsorships), also taking into account the possible reputational involvement. This interpretation would be in line with the principles dictated by the Italian DPA in the "Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes" dated 17/09/15.
- **Processing of judicial data for the purpose of assessing the reliability of candidates and employees**: in certain sectors, employers wishing to evaluate a candidate or employee for the purposes of establishing/continuing an employment relationship may have a legitimate interest in processing the personal data of the data subject in question. This could be as a result of any involvement in crimes that may undermine the reliability of the subject or expose the employer to actual risks

that can undermine - for example in the case of financial intermediaries - the system of internal controls (for example in the case of a bank that hires a terrorist). In both the above cases, the 3 prerequisites for recourse to legitimate interest would be considered satisfied, not least the reasonable expectation of the data subject to whom the data, including judicial data, refers.

Finally, in addition to the processing of personal data for internal administrative purposes within a business group, we recommend that the EDPB **includes additional scenarios of data sharing within a group where legitimate interest may provide a valid legal basis for processing**. These examples could include:

- The sharing of data between the mother company of a group of undertakings and its affiliates for the dual purpose of drafting good management reports, and thus help the administration of the financial institution, but also producing reports required by local regulators.
- **Credit risk monitoring**: the sharing of data within a Group for the purpose of credit risk monitoring may also rely on the legal basis of legitimate interest. Such sharing would have the dual purpose of preventing and mitigating the risk in question, on both the customer side and on the side of companies belonging to the same Group and Parent Company. Such sharing would be in line with the expectations of a person who is already a customer of a company belonging to a Group that asks to enter into a relationship with another company of the same Group that reasonably expects that the assessments of its solvency and reliability will take into consideration data coming not only from the Exchanges and SICs, but also and above all by the performance of the relationships already established with other companies of the Group. Such sharing would also have a benefit in terms of improving credit recovery actions. We would like to point out that developments at national level have also begun to acknowledge reliance on legitimate interest for credit risk monitoring purposes. For example, in the opinion of the Italian DPA, controllers may rely on legitimate interest as a legal basis for the processing of personal data for the purposes of risk monitoring of credit and over-indebtedness; so much so that the legal basis for the processing in the case of access to and contribution to the SICs (both in the case of positive and negative reports) is now the legitimate interest. Among other things, the sharing in this sense also seems to be in line with the EBA Guidelines.
- There are also situations in which having to share data is not a mere legitimate interest but an expectation of regulators, such as the ECB. Banks have little choice but to share data to demonstrate the regulator that they are in control of the risks that by law need to be managed, taking into account the principles of data minimisation, etc. Where such need for data to be shared cannot be found in a clear legal obligation or imposition/expectation of the regulator, legitimate interest should be relied on.

6. Processing for the purpose of ensuring network and information security

We would like to bring to the attention of the EDPB the fact that, as fraud and cyber threats continue to evolve, organisations are continuously adapting their security measures and associated data processing practices. We are of the opinion that the EDPB should acknowledge this dynamic environment and ensure that the Guidelines are flexible enough to address new and emerging threats as they arise. This recognition is crucial for

maintaining robust security protocols that can effectively counteract the sophisticated tactics employed by cybercriminals.

Paragraph 127 states that "*security cannot justify an excessive processing of personal data*". It is unclear why this was added on top of the already existing principle of the respect of necessity and balance of interests.

In terms of security, with particular reference to the protection of company assets as well as the protection of data processed by the Data Controller in terms of prevention and mitigation of data breaches (including data breaches), it may be appropriate to include among the hypotheses of legitimate interest the installation of scouting systems aimed at intercepting attempts to "leak" data to external email addresses. These systems that are not aimed at remote control of the worker, but at making the supervision more efficient when preventing illegal data processing, violation of banking secrecy and, last but not least, safeguarding company assets.

7. Transmission of personal data to competent authorities

7.1 Indicating possible criminal acts or threats to public security to competent authorities

We have reservations with **Example 8**, which states that "*This processing could be based on Article 6(1)(f) GDPR if, in each specific case, it is necessary and the legitimate interest pursued by the controller to indicate possible criminal acts or threats to public security is not outweighed by the interests and rights and freedoms of concerned data subjects*." In this or similar cases, it would not be appropriate to take into account the purpose of protecting public safety, a security that - in many cases - is also an element in favor of the interested parties themselves.

7.2 Requests from and disclosure to third country authorities

1. The Guidelines appear to suggest that legitimate interest would rarely be the correct legal basis to rely upon for processing personal data in response to a request from a third country authority, but that it may be the correct lawful basis in a case where the third country authority might be subject to third country law, and non-compliance with the request would entail sanctions under foreign law. In practice, we do not often see firms relying on public or vital interests for this processing and firms do have a strong legitimate interest in complying with third country requests. **Failure to comply can result in significant financial penalties, impede the combating of international criminal activity, and could result in the financial institution losing its licence in the third country, amounting to reputational damage**.

ENDS

For more information:
Rachele Ceraulo
Project Coordinator – 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

www.ebf.eu @EBFeu

www.ebf.eu