23 January 2018

EBF_030536

EUROPEAN BANKING FEDERATION'S COMMENTS ON THE ARTICLE 29 WORKING PARTY GUIDELINES ON TRANSPARENCY (WP260)

The European Banking Federation (EBF) welcomes the opportunity to comment on the work of the Article 29 Working Party (WP29) considering its relevance for the whole banking industry. The WP29 Guidelines are highly appreciated and we believe it is of utmost importance that the final Guidelines both follow the direction set in the General Data Protection Regulation (GDPR) and are easily applicable across industries and across Member States.

As stated by the European Parliament, "the goal [of the GDPR] is a more coherent data protection framework at EU-level, backed by strong enforcement procedures. Intended as a wide-ranging and farsighted reform to improve and harmonise data protection in the digital age, the regulation updates most of the existing rules and introduces new ones". It is thus important to have these goals in mind when developing (and applying) the GDPR Guidelines.

Therefore, the established principles of data and consumer protection should be at the core of the Guidelines, which need to be applied in a dynamic, innovative and effective way. The GDPR also needs to fulfil the objective to enhance the internal market and citizens' trust in the digital single market, fostered through legal certainty and legal consistency across Member States.

Key points:

- **A technology-neutral and future-proof approach should be preferred.** As tools, techniques and mechanisms constituting appropriate measures to provide information to data subjects are constantly evolving, it is imperative that the Guidelines are adjusted so that they take a **technology-neutral and future-proof approach in order to allow controllers to assess the most efficient way to inform data subjects of their rights**.

- **To decrease information overflow, emphasis should be placed on the controller's expertise to decide the most appropriate way to allow data subjects to exercise their rights.** A multi-layered approach with referrals to

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

extra information on "clickable" texts or referrals to the general privacy statement of the given institution should be recognized as best practice. This will not only provide controllers with the opportunity to determine the most appropriate way for data subjects to exercise their rights, but **help data subjects understand more thoroughly and fully exercise their rights**.

- **Avoid confusion and misunderstanding by placing data subjects at the centre.** As stated in Article 12 of the GDPR, the information provided to the data subjects needs to be concise, clear and intelligible. It is therefore essential to listen to the needs of consumers in a specific sector and to find **the best way to empower citizens without overloading or burdening them with too much information.**

- **Article 29 Working Party Guidelines need to be aligned with the GDPR** and recommendations should only be provided when a "new requirement" is clearly in line with the GDPR and in the clear interest of data subjects. Both smaller, medium and large international controller groups with sophisticated and diverse processing activities need to be able to adhere to these recommendations. In their present format the recommendations only cater to controllers of basic activities.

EBF comments

Elements of transparency under the GDPR (page 7)

"Concise, transparent, intelligible and easily accessible" (page 7)

In paragraph 8, it is specified that the information provided should be intelligible, defined as understandable "*by an average member of the intended audience*". Intelligible information is, under normal circumstances, understood in the sense that an average informed person is able to comprehend this piece of information. Such an average informed person is normally understood as any person rather than a person of a certain audience.

Moreover, by not only referring to the 'intended audience' but by also defining who is part of such an intended audience and how to assess it, **the WP29 goes beyond the wording of the GDPR and the section should be amended**. To require specific, tailor-made information for different audience groups would create uncertainty about the level required from an audience group. In addition, if the information were tailored for a certain kind of audience, data subjects who, in the controller's view, are not a part of that group would be at an informational disadvantage.

Additionally, the WP29 requires regular reviews to ensure that the actual audience and intended audience correspond. To review regularly who the actual audience is would require further data processing, contradicting one of the basic ideas of the GDPR: data minimization. Such reviews could also be seen as profiling and could lead to unnecessary discrimination or other intrusions in the rights and freedoms of the data subjects, especially for cases where the audience can be very large and differentiated.

Paragraph 9 states that a good practice would be to "*spell out the most important consequences of the processing activity*". However, articles 13 and 14 already provide detailed and adequate information for data subjects to be able to claim their rights. Therefore, there is a high probability of confusing data subjects by providing them with excess information.

In addition, by stating that "*a description of the consequences of the processing should not simply rely on innocuous and predictable "best case" examples of data processing*", the WP29 also recommends a description of potential 'worst case' scenarios. We suggest deleting the best practice described by the WP29 in this paragraph. Examples of unlikely consequences risk confusing data subjects who could believe that the "worst case scenarios" are likely to happen. This will also ensure that this paragraph provides concrete guidance. Furthermore, this best practice seems to go beyond what is prescribed by the GDPR. According to Article 13.2, controllers shall only provide information on the consequences of processing where it relates to automated decision-making (Article 13.2 (f)). At the very least, the fact that this represents a best practice (and not an obligation) should be emphasised and **it needs to clarified that this is not the intention of the**

WP29 and that the explanation of the consequences, if such descriptions are suitable, should relate only to the likely effect of the intended processing.

The example in paragraph 10 (page 8) details that privacy statements shall be accessible from each individual page of website. This is an unnecessary obligation since the average data subject is accustomed to navigating through menus and similar modalities where clear links to the privacy pages can be provided. Technical development could also provide for other manners of providing information and the Guidelines should allow this. As stated above, tools, techniques and mechanisms constituting appropriate measures to provide information to data subjects are constantly evolving. It is imperative that the Guidelines are adjusted so that they take a technology-neutral and future-proof approach in order to allow controllers to best assess the most efficient way to inform data subjects of their rights. The WP29 should also allow for a wider spectrum of titles of privacy statements since the provided examples do not take into consideration diverse jurisdictions' specific needs when it comes to language and cultural differences. Furthermore, this example is formulated in a way that is too general. We would suggest redrafting it.

EBF suggestions for amendments:

WP29 Guidelines, page 7, paragraph 8:

"8. The requirement that information is "intelligible" means that it should be understood by an average member of the ~~*intended*~~ *audience.* ~~*This means that the controller needs to first identify the intended audience and ascertain the average member's level of understanding. As the intended audience may, however, differ from the actual audience, the controller should also regularly check whether the information/ communication is still tailored to the actual audience (in particular where it comprises children), and make adjustments if necessary.*~~ *Controllers can demonstrate their compliance with the transparency principle by testing the intelligibility of the information and effectiveness of user interfaces/ notices/ policies etc. through user panels."*

WP29 Guidelines, page 8, paragraph 9:

Option 1:
"~~*As a best practice, in particular for complex, technical or unexpected data processing, the WP29 position is that controllers should not only provide the prescribed information under Articles 13 and 14, but also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? Such a description of the consequences of the processing should not simply rely on innocuous and predictable "best case" examples of data processing, but should provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to protection of their personal data.*~~*"*

Option 2:
"As a best practice, in particular for complex, technical or unexpected data processing, the WP29 position is that controllers should not only provide the prescribed information under Articles 13 and 14, but also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? Such a description of the consequences of the processing, ***if such descriptions are suitable****, should* ***relate only to the likely effect of the intended processing*** ~~***not simply rely on innocuous and predictable "best case" examples of data processing, but should provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to protection of their personal data***~~*."*

WP29 Guidelines, page 8, paragraph 10:

*"****Example***

~~***Every***~~ ***An*** *organisation that maintains a website* ~~***should***~~ ***can*** *publish a privacy statement/ notice on the website. A link to this privacy statement/ notice* ~~***should***~~ ***can*** *be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"* ***although the exact method used and terms should be left to the discretion of the controller to suit language and cultural differences****. Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.*

For ***an*** *app*~~***s***~~*, the necessary information* ~~***should***~~ ***can*** *also be made available from an online store prior to download.* ~~***Once the app is installed, the information should never be more than "two taps away". Generally speaking, this means that t***~~***T****he menu functionality often used in apps* ~~***should always***~~ ***can*** *include a "Privacy"/ "Data Protection" option* ***although the exact method used and terms should be left to the discretion of the controller to suit language and cultural differences****.*

~~***WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.***~~*"*

"Clear and plain language" (page 9)

The examples accompanying paragraph 11 raise the concern of their interaction with the concept of a multi-layered approach. It is of the utmost importance to ensure that data subjects fully understand the information provided to them. As stated above in our response, this is best achieved by avoiding overburdening them with too much information or information that could lead them to have an incorrect understanding about the intended processing activity.

As such, a multi-layered approach with referrals to extra information on "clickable" texts or referrals to the general privacy statement of the given financial institution should be recognized as a best practice. This will not only provide full liberty to controllers to decide what is the most appropriate way to allow data subjects to exercise their rights but it will also help them to understand more thoroughly and exercise their rights fully.

However, in its examples (page 9), the WP29 states that it considers these phrases as '*not sufficiently clear'*. It should be the responsibility of the controller to decide on the choice of words and manners of expressing the processing activity. Also, these phrases, as used in the example, could be considered clear enough as 'first layer' information. It may be possible for the data subject to inquire more about the purposes of the processing, if he or she wishes to do so.

In addition, we do not agree with the WP29 which states that the sentence "*[w]e may use your personal data to develop new services*" is "*not sufficiently clear*" since "*it is unclear what the services are or how the data will help develop them*". Indeed, we would like to point out that when new services are developed, especially in early stages, you do not necessarily know exactly how they will look and which data will be relevant to bring about such development, as this is likely to change at various stages during the development phases of a new product or services.

It should be deemed sufficient to inform the data subject that data will be used for the development of new products. It should also be made clear that the firm, and any other controller or processor, have the obligation to observe all principles of the GDPR when developing new products. If, in the development of a new product, the outcome of the risk analysis is that further information should be provided or that consent should be required, this needs to be done. Requiring to inform the data subject every time their data might be processed for the development of a certain product would be tiresome for the data subject.

Providing information to children (page 9)

The drafting of paragraph 13 (page 10) is unclear. Indeed, it reads that "*the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects"*. This, in conjunction with paragraph 17 of the Guidelines (page 12), seems to suggest that all disabilities of the possible public need to be taken into account. This requirement goes beyond what is stipulated in the GDPR. Moreover, it should be noted that according to national law[1], protectors can be provided to person with disabilities. This should thus be left to national consumer protection rules.

[1] Notably, but not only, following the implementation of the United Nations Convention on the Rights of Persons with Disabilities of 13 December 2006 (https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/convention-on-the-rights-of-persons-with-disabilities-2.html - last accessed 23 January 2018)

Information to be provided to the data subject – Articles 13 & 14 (page 12)

"Appropriate measures" (page 12)

In paragraph 22 (page 13), the WP29 states that "*[b]eing accountable as regards transparency applies (...) when changing the contents/ conditions of existing privacy statements/ notices*". This part of the Guidelines seems unclear as to which type of changes would be deemed relevant enough to trigger the process of communicating them to the data subject as the WP29 only refers to "*subsequent changes*". As stated above, over-soliciting data subjects with information will be counter-productive especially if every change is required to be communicated. It should then be up to each controller to decide when and in what manner such notifications are to be made, in order for the notification to adhere to the requirements in Article 12, and in particular to the requirement to maintain a concise stream of information to the benefit of data subjects.

The paragraph continues and states that "*(...) the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them*". This places an unnecessary heavy burden on controllers that need to cater for various categories of data subjects and will require additional processing of personal data.

Additionally, we are of the view that this paragraph includes a new obligation, going beyond the requirements of the GDPR, when stating that "*a notification of changes should always be communicated by way of an appropriate modality (e.g. email/ hard copy letter etc.)*". The manner, channel and technical solution for communicating should be at the discretion of the controller who is best suited to conclude a suitable method adapted to its customers. The paragraph should be amended to refer clearly to this point.

EBF suggestions for amendments:

WP29 Guidelines, page 13, paragraph 22:

"Being accountable as regards transparency applies not only at the point of collection of personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents/ conditions of existing privacy statements/ notices. ~~***The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent changes to this statement.***~~ *Since most existing customers or users will only glance over communications of changes to privacy statements/ notices, the controller should take* ~~***all***~~ *measures* ***it deems*** *necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means for example that a notification of changes should always be communicated by way of a*~~***n***~~ ***modality deemed*** *appropriate* ***by the controller*** ~~***modality (e.g. email/ hard copy letter etc.) specifically devoted to those changes (e.g. not together with direct marketing content)***~~*, with such a*

communication meeting the Article 12 requirements of being concise, intelligible, easily accessible and using clear and plain language."

Timing for provision of information (page 14)

In paragraph 24, the WP29 gives an interpretation of Article 14.3 of the GDPR and extends the one month time limit provided for Article 14.3(a) to Article 14.3(b) and Article 14.3(c). We are of the view that this interpretation goes beyond the GDPR as the Regulation distinguishes different hypotheses and the one month time limit is envisaged only in the first case, under letter (a). **We would thus suggest redrafting paragraph 24 of the Guidelines to reflect this point**.

In paragraph 25, the WP29 recommends that "*data controllers should provide the information to data subjects well in advance of the stipulated time limits*" (page 15). This sentence should be deleted as it goes far beyond what is expressly prescribed by the GDPR which sets time limits in order to ensure data subjects are appropriately "*made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing*" (GDPR, Recital 39).

Timing of notification of changes to Article 13 and 14 information (page 15)

Paragraph 27 states that "*compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before*" (page 16). The sentence should be deleted since it is clear that controllers always need to adhere to all requirements in the GDPR and not just the principle of transparency

It is our understanding that, in paragraph 28 (page 16), the WP29 guidance is going beyond obligations under the Regulation. The controller does not, according to the GDPR, have an obligation to inform the data subject about issues of which he or she is already aware. In addition, this would not, in practice, be feasible without creating excessive burden for both controllers and data subjects. Furthermore, the data subject would not expect to be notified without reason. As stated above, it is imperative to identify the data subjects' information needs and identify a suitable way to empower data subjects without overloading or burdening them with excess information. We thus suggest deleting this paragraph.

EBF suggestions for amendments:

WP29 Guidelines, page 16, paragraph 27:

"Further, WP29's position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. ***~~However, compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before.~~*** *WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations."*

WP29 guideline, page 16, paragraph 28:

*"****~~28. Additionally, even when transparency information (e.g. contained in a privacy statement/ notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. For those situations, where the data processing occurs on an ongoing basis, in order to ensure fairness of the processing, the controller should reacquaint data subjects with the scope of the data processing, for example by way of reminder of the privacy statement/ notice notified at appropriate intervals."~~***

Modalities – format of information provision (page 16)

It is our view that paragraph 29 should be deleted. It is not unreasonable to require active engagement by the data subject. Semantically, to our understanding, a layered internet page (recommended by the WP29) still needs the data subject to *actively* access the page. This conflicts with the statement in paragraph 29 that the data subject should not need to take any active steps.

Furthermore, the assertion that "*[t]he data subject must not have to take active steps to seek the information covered by these articles*" (page 16) seems excessive. Indeed, the Court of Justice of the European Union (see judgment of 25 January 2017, Case C-375/15[2]) considers that information transmitted by a bank to its customers on a messaging platform available to them on the bank's website is considered "*provided*" (within the meaning of the first Payment Service Directive) if this transmission is accompanied by an "*active behaviour*" from the bank's side (for instance, informing the consumer of the existence and availability of this information on a given website by sending an email). The

[2] ECJ judgment on case C-375/15: http://curia.europa.eu/juris/document/document.jsf?text=&docid=187125&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=902885 (accessed on 11 January 2018)

condition to an "*active step*" of the controller should therefore not be limited to the "*provision*" of the information. We would thus suggest deleting paragraph 29.

EBF suggestion for amendment:

WP29 Guidelines, page 16, paragraph 29:

"~~***29. Both Article 13 and 14 refer to the obligation on the data controller to "provide the data subject with all of the following information…" The operative word here is "provide". This means that the data controller must take active steps to furnish the information in question to the data subject. The data subject must not have to take active steps to seek the information covered by these articles or find it amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 10 illustrates this point.***~~"

Information related to further processing (page 20)

We believe **paragraph 40** (page 21) provides an additional obligation when the WP29 states that "*data controllers should provide data subjects with further information on the compatibility analysis carried out under Article 6.4*". Indeed, this is not a requirement present in either Article 13 or 14 of the GDPR. The addition risks increasing the data subject's information-fatigue; even more so, considering that explaining this assessment (to all possible audiences) would most likely be complex and lengthy without further empowering the data subjects. Hence, we believe that **the text should be removed**.

Lastly, it is our understanding that, in **paragraph 41 (page 21)**, the WP29 is again expanding the obligations under the Regulation when it states that "*a reasonable period should occur between the notification and the processing commencing rather than an immediate start to the processing upon notification being received by the data subject*". The GDPR already provides for when information is to be provided and it is not reasonable to expect a controller to notify before the timeline and limits present in the GDPR. We would **thus suggest deleting the end of the paragraph, starting at the sentence quoted above**.

Visualisation tools (page 21)

Icons (page 22)

We welcome the acknowledgment in the Guidelines that, "*in line with Recital 166, the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in*

this context" (paragraph 45, page 23). It is indeed important to take the time to reflect on standardized icons and look at the real needs of both the market and the data subjects.

There is a risk that data subjects will not understand anymore what the icons are meant to state. It could also be detrimental to controllers because an icon could be misleading. In addition, it should be noted that a pictogram or icon may not be interpreted in the same manner from one country to another due to cultural differences. **Consequently, the content of information should prevail on the referred icons**.

Furthermore, the development of icons is not an obligation under the GDPR and the development of any code of icons should be left to the controllers.

Exceptions to the obligation to provide information (page 24)

Article 13 exceptions (page 24)

In its example pages 24 and 25, the WP29 states that "*a matter of best practice however, all of this information should be provided to the data subject again*" ("*this information*" refers to *"certain Article 13.1 and 13.2 information about the processing of the telephone number"* and *"other information that the individual already has from 6 months ago and which has not since changed")*. We would like to point out that this best practice as described by the WP29 risks increasing information fatigue among data subjects. **We would suggest amending or deleting this part.** A link to the privacy notice can be provided as a best practice but it should be made clear that there is no obligation to do so.

"Disproportionate effort" (page 27)

The example given on page 27 seems too strict. It only covers a case where Article 89 of the GDPR (which is explicitly stated in Article 14) is relevant but does not cover examples where this is not the case. Further examples would be welcomed.

For instance, in the banking sector, cases where an institution sells credits in blocks, in cases of securitization regulated by national banking law, could be taken as an example. Informing each and every debtor individually before proceeding to the sale would result in administrative costs and commitments manifestly disproportionate to the protected right.

This has been recognized by some Data Protection Authorities (DPAs) as being an example of disproportionate effort (under the framework of the Directive). Some DPAs confirmed[3] that in such cases, the information required can be communicated in a non-individualized form as a first step, provided that the information is made known in such a way as to allow the unambiguous identification (according to objective and predetermined parameters) of

[3] See for instance, Opinion n. 1392461, http://www.qpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1392461 (last accessed 18 January 2018)

the debit positions being sold; and then, as a second step, by means of the subsequent communication to the debtors, at the first possible opportunity.

Transparency and data breaches (page 30)

In paragraph 62 (page 30), the WP29 refers to its Guidelines on Data Breach Notification and states that "*a data controller's obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12*". The reference to Article 12 for data breach notification seems to go beyond the GDPR as this risks to confuse the contents and the obligations under Article 33 ("*Notification of a personal data breach to the supervisory authority*") with the contents and the obligations of the abovementioned Article. We would thus suggest deleting this reference.

EBF suggestion for amendment:

WP29 Guidelines, page 30, paragraph 62:

"62. WP29 has produced separate Guidelines on Data Breaches but for the purposes of these Guidelines, ~~***a data controller's obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12. T***~~ *the communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14."*

Schedule – Information that must be provided to a data subject under Article 13 or Article 14 (page 31)

Please note that all comments below refer to the column titled "*WP29 Comments on information requirement".*

Where legitimate interests (Article 6.1(f)) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party (page 31)

We believe the WP29 goes beyond what is prescribed in the GDPR when it states that "*[a]s a matter of best practice, the data controller should also provide the data subject with the information from the balancing test*". Under the GDPR, the exact calculations made by the controller do not need to be provided to the data subject.

As stated above in our comments, it is of the utmost importance to prevent and minimise information fatigue and this best practice risks disengaging data subjects. We would thus suggest deleting this part of recommendation.

EBF suggestion for amendment:

WP29 Guidelines, page 31, line 5, "WP29 Comments on information requirement":

"The specific interest in question must be identified for the benefit of the data subject. ~~***As a matter of best practice, the data controller should also provide the data subject with the information from the balancing test, which should have been carried out by the data controller to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data."***~~

Recipients (or categories of recipients) of the personal data (page 32)

The aim, to ensure that data subjects fully understand how their personal data is being and will be used, is of great importance. Hence, it is important for them to know if their personal data will be shared with third parties. It is doubtful that they would gain more by being provided with the name of the exact individual recipients that will receive the data compared to being provided with categories of recipients. This is even more the case in the financial industry. We note that banks can often engage hundreds of processors. Providing such a list to data subjects would increase the risk of information fatigue. What is more, the processors/ vendors can change frequently. This could result either in a list becoming inaccurate or data subjects being bothered with constant updates as every change in the list would have to be notified; thus overburdening them.

Hence, the WP29 should make clear that providing a list with the name of every single processor is not an obligation.

Details of transfers to third countries, the fact of same and the details of the relevant safeguards (including the existence or absence of a Commission adequacy decision) and the means to obtain a copy of them or where they have been made available (page 33)

In its recommendations, the WP29 states that the "*relevant GDPR article permitting the transfer and the corresponding mechanism*" should be specified. We would suggest deleting this reference since that kind of information and level of detail will not provide understandable information, in line with Article 12. This recommendation runs contrary to the obligation to "*provide any information (...) relating to the processing to the data subject in a concise, transparent, intelligible and easily accessible form*" (Article 12 GDPR), especially as the WP29 interprets 'intelligible' as meaning understandable by an average person of the targeted audience. Disclosing the exact article and corresponding mechanism would lead to providing a text that would be more understandable for data protection lawyers than anybody else. **This recommendation should therefore either be deleted or amended to ensure it fully respects the obligation under Article 12.**

Furthermore, the WP29 continues by saying that "*the information should explicitly mention all third countries to which the data will be transferred*". As stated above, financial institutions often engage hundreds of processors which can be located in different countries and these can change frequently. Providing a list of third-countries to which data will be transferred, and thus constantly sending updates to data subjects given frequently changing processors/ vendors, will be counter-productive as every change in the list would have to be notified; thus overburdening data subjects. Furthermore, it may be questioned if it is in the interest of the data subject to have that exact information. We would suggest deleting this recommendation.

EBF suggestions for amendment:

WP29 Guidelines, page 33, line 1, "WP29 Comments on information requirement":

"~~***The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45 / binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified.***~~ *Where possible, a link to the mechanism used or information on where and how the relevant document may be accessed or obtained should also be provided.* ~~***In accordance with the principle of fairness, the information should explicitly mention all third countries to which the data will be transferred.***~~"

The storage period (or if not possible, criteria used to determine that period) (page 33)

In the financial sector, companies must often hold personal data for various reasons and purposes. These include multiple legal and regulatory compliance purposes. This leads to firms holding many types of personal data for a varying amount of time. Drafting a full retention schedule would therefore not only prove extremely complex but unlikely to be useful to data subjects. On the contrary, this could confuse him or her and lead to increase information-fatigue.

The WP29 should thus encourage a more flexible approach and allow more general descriptions.

The rights of the data subject to access; rectification; erasure; restriction on processing; objection to processing and portability (page 34)

In this paragraph, the WP29 recommends that "*[t]he specific source of the data should be provided unless it is not possible to do so*". Although we agree that it is important to provide data subjects with a description of data sources, we worry that providing a list of each individual source risks further disengagement from the data subjects.

This is further reinforced by the fact that, if such a list of individual sources is provided, every change in it would have to be notified to the data subject. This could potentially lead to a large amount of update notification being sent to the data subject, placing a heavy burden on small and medium-sized controllers.

It would be preferable to amend this part of the Guidelines by allowing a description of the types of data sources with the possibility to request more information, including a list of individual sources. This would enable data subjects to be fully empowered by providing them information that is useful while minimising the risk of overburdening them.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Hélène BENOIST
Policy Adviser
Digital & Retail
h.benoist@ebf.eu
+32 2 508 37 35

www.ebf.eu