23 January 2018

EBF_030527

EUROPEAN BANKING FEDERATION'S COMMENTS ON THE ARTICLE 29 WORKING PARTY GUIDELINES ON CONSENT (WP259)

EBF key points:

- **Supporting the clarifications on consent provided by the WP29.** The European Banking Federation (EBF) welcomes the Article 29 Data Protection Authority (hereafter 'WP29') Guidelines on consent which is one of the central point of the General Data Protection Regulation (GDPR).

- **Avoiding consent and information fatigue**. The banking sector supports the main objectives of the GDPR, as to increased transparency regarding personal data processing and empowering data subjects. However, it is important to avoid overburdening data subjects with too much information on too many occasions. An appropriate level of granularity needs to be found that does not lead the data subject to be nudged and bothered constantly, as this risks causing them to disengage from data protection issues.

- **A need to ensure a consistent consent framework**. The framework for consent needs to reflect that each industry has particular challenges and differences that impact the appropriate manner in which to implement consent under the GDPR. For instance, certain provisions in these Guidelines raise questions as to the potential consequences on the lawfulness of consents given under the Second Payment Service Directive (Directive (EU) 2015/2366 – PSD2) and the Markets in Financial Instruments (Directive 2014/65/EU - MiFID II).

- **Future-proofing and ensuring technology-neutrality.** Tools, techniques and mechanisms constituting appropriate measures to obtain consent from the data subjects are constantly evolving. Therefore, it is important to take a technology-neutral approach in order to allow controllers to best assess the most efficient way to inform data subjects and obtain consent.

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

EBF comments

Introduction (page 4)

The EBF welcomes the reminder that consent is only one of the six legal grounds provided for by the GDPR when the WP29 writes that "*[w]hen initiating activities that involve processing of personal data, a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead*". Even though consent is a key concept, at the heart of the GDPR, we believe it is important to remember that it may not always be the most suited ground for processing.

Equally, we welcome the efforts of the WP29 to clarify the articulation of the notion of consent under the GDPR and other texts. The Guidelines notably reference the ePrivacy Directive as well as its current review (page 5 of the Guidelines). Similar analysis for the notion of consent under such texts as the Second Payment Service Directive (Directive (EU) 2015/2366 – PSD2) and the Markets in Financial Instruments (Directive 2014/65/EU - MiFID II) would be welcome in due course. These texts serve as examples of where potential conflicts can arise regarding the discipline of consent given under these frameworks.

It is important that the framework for consent under the GDPR is aligned with other recent legislation at EU level. It should thus be reflected that each industry has particular challenges and differences that impact the appropriate manner in which to implement consent under the GDPR. This is particularly important when the WP29 states later in its Guidelines that "*[if] consent is bundled-up as a non-negotiable part of terms and conditions it is presumed not to have been freely given*". The consequences on consent according to the two above-mentioned texts are unclear and careful consideration, in conjunction with industry consultation, will be required.

Elements of valid consent (page 6)

Free/ Freely given (page 6)

Although it is important to note that consent should not be coerced, in certain circumstances, consent may need to be asked, for example because of a law that requires it, and if it is not granted, the consequence may be that the client will not be able to enjoy certain services. We believe then that the sentence "*consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment*" (page 6, last paragraph) should be amended and nuanced in order to reflect and clarify that there exist situations to which this sentence cannot apply.

This will be the case, for instance, of a data subject requesting certain mortgage products. The institution providing the mortgage may need to ask, because the law requires it, for consent to process health-related data in order to better assess the long-term risks of

lending money and the data subject's ability to repay at a future date. Indeed, in some Member States, the Financial Supervisory Authority requires financial institutions to process health-related data as part of their credit-worthiness assessment. In such a situation, should the data subject refuse to grant its consent, the financial institution has two choices: either take a 'worse-case scenario' approach which may lead the data subject to paying more as the bank cannot properly assess his or her solvability, or refusing the mortgage altogether. Although consent needs to be asked, it should be noted that in some situations, a refusal to grant consent could lead to a data subject being refused a service or product, or prove detrimental to him or her, as it may otherwise be impossible to provide the mortgage[1] responsibly.

EBF suggestion for amendment:

WP29 Guidelines, Page 6, last paragraph:

"The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, ***in some situations,*** *consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.* ***The WP29 acknowledges that there exists situations in which a service or product could not be provided, or not be provided without detriment, to a data subject, should the latter refuse to grant consent (see example 1 below). This arises in particular when special category personal data are necessary for the provision of a service.*** *The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.*

[Example 1] - new
A data subject wishes to obtain a mortgage in a bank. The bank asks for the consent of the consumer to process his or her health-related data as part of its credit-worthiness assessment in order to evaluate the data subject's solvability and ability to repay the mortgage in the future. In this situation, should the data subject refuse to grant its consent, the bank has two options: either take a 'worse-case scenario' approach which may lead the data subject to pay more as the bank cannot properly assess the data subject's capacity to repay in the future, or refuse the mortgage altogether. Although consent needs to be asked, it should be noted that in some situations, a refusal to grant consent could lead to a data subject being refused a service or product, or prove detrimental to him or her, as it may otherwise be impossible to provide the mortgage responsibly.*"*

[1] For instance, in the United-Kingdom, the Financial Conduct Authority's "*Mortgage and Home Finance: Conduct of Business sourcebook*" (MCOB) requires that "*[w]hen a firm assesses whether the equity release transaction is appropriate to the needs and circumstances of the customer for the purposes of MCOB 8.5A.5 R, the factors it must consider include the following: (...) (5) the customer's health and life expectancy;*" (MCOB 8.5A.6 (f): https://www.handbook.fca.org.uk/handbook/MCOB/8/5A.html (last accessed 17 January 2018)).

Imbalance of power (page 7)

In its Guidelines, the WP29 states that "*[a]n imbalance of power also occurs in the employment context*" (page 8, paragraph 1). There is a need to nuance the sentence as situations in which an employee can give his or her consent "freely", even if the request comes from his or her employer, are possible – as the WP29 states later in its Guidelines (page 8, paragraph 2). For instance, the word "*may*" could be inserted to nuance the sentence.

In addition, we suggest making a reference to the possibility for an employer to rely on other legal basis, provided the safeguards established by the GDPR are in place.

EBF suggestion for amendment:

WP29 Guidelines, page 8, paragraph 1:

*"An imbalance of power **may** also occur~~s~~ in the employment context".*

Conditionality (page 8)

In relation to the term 'necessary for the performance of a contract', the WP29's Guidelines read *"[t]his may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid"* (page 9, paragraph 4).

These examples seem very basic. In the banking and insurance sectors, the processing of data for the performance of a contract is most of the time a lot more complex and, for instance, some non-financial data may be relevant for the purpose of concluding an insurance policy or to grant financing. It would thus be more appropriate in our view to extend this concept.

Therefore, a first step could be to delete the word "*may*" in the above-quoted sentences as the examples provided are basic and evident.

Moreover, we would suggest modifying the example 6, page 10 of the Guidelines. As currently drafted, it is misleading and does not reflect the practice of banks. Under certain circumstances, data *may* be processed for marketing purposes on the ground of legitimate interest. However, banks do not make their services or products contingent on whether a client has granted his or her consent for the processing of data that are not necessary for the performance of a contract between a bank and its customer. It should also be noted that this example could be generalised to other industries and sectors, and should not only target financial institutions.

Example 6 (page 10) should be modified in order to make it clear that there also exist other purposes. This could be achieved by amending the amendment as follows: "*A bank asks customers for consent to use their payment details for* ***~~marketing~~*** *purposes* ***outside 'legitimate interest' or 'performance of a contract'***".

In the fourth paragraph of page 10, the WP29 states that "*[t]he controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service that does not involve consenting to data use for additional purposes on the other. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However,* ***both services need to be genuinely equivalent, including no further costs***".

One of the main reasons to obtain and process more data is to provide added-value and offer enhanced services to customers. These products or services then become sort of 'upgraded' thanks to the personalization offered by the data obtained. Offering a similar product or service without collecting data could then be seen as a "'degraded' service" as crucial information to provide personalization would be missing. The paragraph quoted above should thus be amended to reflect this point.

EBF suggestions for amendments:

WP29 Guidelines, page 9, paragraph 4:

"This ***~~may~~*** *include****s****, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground* ***~~may~~*** *allow****s****, for example, the processing of salary information and bank account details so that wages can be paid"*

WP29 Guidelines, page 10:

"[Example 6]
A bank asks customers for consent to use their payment details for ***~~marketing~~*** *purposes* ***outside 'legitimate interest' or 'performance of a contract'.*** *This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or an increase of the fee, consent cannot be freely given or revoked."*

Granularity (page 11)

As currently written, this part of the Guidelines gives the impression that consent is the only ground on which the processing of data for such purposes is allowed.

Similarly, the example 7 (page 11) does not seem fully complete or accurate. It states that "*[w]ithin the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consent for these two separate purposes therefore the consent will not be valid*". The basis for this processing could be 'legitimate interest', for instance in the context of fighting fraud or 'legal obligation' when performing 'Know-Your-Customer' activities. We would thus suggest complementing and clarifying this example. In this light, it would be appreciated if the WP29 would add a footnote to the text as suggested in our amendment below.

EBF suggestion for amendment:

WP29 Guidelines, page 11, example 7:

"[Example 7]
Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies[1] within their group. This consent is not granular as there is no separate consents for these two separate purposes therefore the consent will not be valid.

(...)

_____

[1]. This example does not imply that consent is necessary when a company shares contact details of its customers with other group companies for marketing purposes. Such disclosure could also be based on the legitimate interests of the company provided that the rest of the obligations laid down in the GDPR are abided by. If the group company which receives the contact details of the client in line with the GDPR decides to approach that client, by email for example, this company will have to abide by the ePrivacy Directive."

Specific (page 12)

In its explanation of "*purpose specification as a safeguard against function creep*", the Guidelines state that if "*a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose. The original consent will never legitimise further or new purposes for processing*" (page 12, paragraph 4). We believe a reference to the other legal grounds for processing would be a beneficial addition to this paragraph.

Indeed, it can be that the new purpose is compatible with other purposes where the processing is based on other legitimate grounds. In these cases, consent will not be necessary. Recital 50 of the GDPR specifies that "*the processing of personal data for purposes other than those for which the personal data were initially collected* ***should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected****. In such a case,* ***no legal basis separate from***

that which allowed the collection of the personal data is required". Therefore, a new consent is requested only when the "new" processing is not compatible with the purposes for which the personal data were collected.

Additionally, example 8 (page 12) describes a situation with a totally new purpose which is unlikely to be considered 'compatible'.

EBF suggestion for amendment:

WP29 Guidelines, page 12, paragraph 4:

"If a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose, ***unless the new processing is compatible with the purposes for which the personal data were initially collected****. The original consent will never legitimise further or new purposes for processing* ***which are not compatible within the meaning of Recital 50****."*

Informed (page 13)

Minimum content requirements for consent to be 'informed' (page 13)

The WP29 states that "*in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named*" (page 14, paragraph 1). Although we understand the objectives of the WP29 in these Guidelines, it should be enough to keep an up-to-date list of all these organisations and to make it available to customers upon request. It should be noted that the amount of information with which to provide customers is already substantial. Overburdening data subjects with information should be avoided.

Unambiguous indication of wishes (page 16)

The "Working Document 02/2013 providing guidance on obtaining consent for cookies", in relation to consent, establishes:

> *"Active behaviour means an action the user may take (…)"*
>
> *"Ensuring that the active behaviour is within close to the location where information is presented is essential to be confident that the user can refer the action to the information prompted"*
>
> *"The user action must be such that, taken in conjunction with the provided information on the use of cookies, it can reasonably be interpreted as indication of his/her wishes."*

> ***"The users should have the opportunity to freely choose** between the option to accept some or all cookies or **to decline all or some cookies** **and to retain the possibility to change the cookie settings in the future**."*

It is our understanding that, among the actions to be implemented in order to obtain the consent of the affected party (as it is clear from Working Document 02/2013), it is possible to use "to decline" mechanisms for certain processing that, together with other actions by the affected party, the responsible party can understand and be sure that the affected party has shown an agreement with the indicated processing.

In this sense, **opt-out mechanisms,** linked to other means that allow to obtain an action/ declaration of agreement by the user (with respect to the processing of their previously informed data), **should not be excluded from the possible techniques used to obtain an unequivocal/ unambiguous consent**, provided that the necessary guarantees are given so that such consent is understood to be validly granted (such as clear and specific information on the treatment subject to consent, possibility of revoking consent, etc.).

In addition, we would suggest deleting the following sentence "*as well as merely proceeding with a service cannot be regarded as an active indication of choice*" (page 16, paragraph 5). As we mentioned above, it is important to remain as technology-neutral as possible. It is very possible to imagine that, in a few years' time, proceeding with a service will be a clear indication of choice if, for instance, a notice takes up the full page. Tools, techniques and mechanisms constituting appropriate ways to obtain consent are constantly evolving. It should thus be stressed that a technology-neutral approach will not only future-proof the Guidelines but also allow controllers to empower data subjects the best way possible without overburdening them.

EBF suggestion for amendment:

WP29 Guidelines, page 16, paragraph 5:

"Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, ***~~as well as merely proceeding with a service~~ cannot be regarded as an active indication of choice.***"

Consent through electronic means (page 17)

Although we welcome the WP29's clarification in this part, we would like to stress, as does the WP29 in other parts of its Guidelines, the importance of appropriately tackling "click-fatigue". There seem to be contradictions between this aim and some of the other requests and requirements presented by the WP29.

In addition, the WP29 states that "*controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged*" (page 18, paragraph 1). It is our understanding that this goes beyond and is contrary to what is envisaged by the GDPR, in Recital 50, which specifies that "*the processing of personal data for purposes other than those for which the personal data were initially collected* ***should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected****. In such a case,* ***no legal basis separate from that which allowed the collection of the personal data is required"***. This aligns with Article 6.4 of the GDPR. Therefore, a new consent is requested only when the "new" processing is not compatible with the purposes for which the personal data were collected.

Obtaining explicit consent (page 18)

Although the WP29 notes that consent is only one of the ways to legitimise the processing of data, in this part, the Guidelines refer to Article 22 of the GDPR by stating that "*explicit consent plays a role (...) in Article 22 on automated individual decision-making, including profiling*" (page 18, paragraph 2). It should be recalled that consent is not the only possible grounds for automated decision-making and we believe the Guidelines should make that point clear as well[2]. We thus propose the amendment below.

On page 19, the WP29 recommends using two-stage verification process as a way to make sure that valid explicit consent is obtained (*e.g.* asking the individual to respond to an email stating "I agree," and then sending him a second verification link by email or SMS to confirm agreement, also known as double opt-in). This goes beyond the requirements of explicit consent in the GDPR. Furthermore, this not only risks overburdening the data subject with consent requests, it also undermines the ability of the Guidelines to be future-proof. As stated above, the most efficient ways to gather consent will evolve as the technology evolves. It is important to take a technology-neutral approach in order to allow controllers to best assess the most efficient way to obtain data subjects' consent. This paragraph should be clearly phrased as a non-compulsory example which allows data processors to structure the consent collection otherwise.

[2] For more details, please see the European Banking Federation's comments on the WP29 Guidelines on automated decision-making – WP251, http://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-Guidelines-on-automated-decision-making-and-profiling.pdf (last accessed 11 January 2018).

EBF suggestions for amendments:

WP29 Guidelines, page 18, footnote 38:

*"[38] In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2~~c~~) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject's explicit consent**, as well as when necessary for entering into, or performance of, a contract between the data subject and a data controller, and when it is authorised by Union or Member State law**. WP29 have produced separate Guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251)."*

WP29 Guidelines, page 19, paragraph 2:

"[Example 14] A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.

Technology will keep on evolving and new ways to obtain consent will be developed by data controllers in the future.

[Example 15] – new
Based on current technologies, ~~T~~t*wo stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement."*

Additional conditions for obtaining valid consent (page 19)

Demonstrate consent (page 19)

The banking sector supports the main objectives of the GDPR, as to increased transparency regarding personal data processing and empowering data subjects.

However, it is important to avoid overburdening data subjects with too much information too often. The WP29 referred to this effect in its Transparency Guidelines. We therefore believe that the WP29 recommendation stating that "*as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights*" (page 20, last paragraph) would be counterproductive and would lead to consent-fatigue on the side of the data subject. An appropriate level of granularity needs to be found.

As stated above in our key messages, we strongly believe that, in order to fully empower data subjects, it is important to avoid consent fatigue. The constant flow of information is not helpful for the data subject, and an excess of information runs the danger of not being read. If the data subject is constantly nudged, there is a risk that he or she will not pay attention to that which he or she is consenting. We therefore suggest the deletion of this provision.

EBF suggestion for amendment:

WP29 Guidelines, page 20, last paragraph:

~~"WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights."~~

Withdrawal of consent (page 21)

The WP29 states that "*[w]here consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort*". We would suggest nuancing this sentence as to better ensure a technology-neutral and future-proof approach while ensuring that the data subject can withdraw consent without undue burden. To reach that goal, we believe that the equivalence between the electronic means used (to obtain and withdraw consent) should not be interpreted in a strict way.

The WP29 states that "*[i]f obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful*" (page 4, paragraph 3). This part on the withdrawal of consent is seen to be too restrictive and does not take into consideration the fact that the processing can be based on more than one lawful basis of processing under Article 6(1), which the WP29 states on page 22 (second paragraph). We would suggest adding this clarification to the guidelines.

In addition, the WP29 recommends that "*controllers assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject*" (page 22, paragraph 3). Controllers must have clear retention schedules but this requirement goes beyond any prescription in the GDPR. We would thus suggest deleting this part.

Furthermore, according to Article 17.1, although a data subject has the right to obtain the erasure of personal data, the deletion of the data is not automatic. We thus propose the following amendments to paragraph 3, page 22.

EBF suggestions for amendment:

WP29 Guidelines, page 22, paragraph 3:

"Besides controller's obligation to delete data that was processed on the basis of consent once that consent is withdrawn ***(except if the processing could be maintained on another lawful basis of processing)****, an individual data subject has the opportunity to request erasure of other data concerning him that still resides with the controller, e.g. on the basis of Article 6(1b). To this end, a data subject should exercise their right to have data erased, as laid down in Article 17(1b) and Recital 65.* ~~***WP29 recommends controllers to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject."***~~

Interaction between consent and other lawful grounds in Article 6 GDPR (page 22)

In this part, the WP29 states that the "*lawful basis cannot be modified in the course of processing*" (page 23). A similar point is made in paragraph 5 of page 22. We would suggest noting that exceptions for new regulations could apply to the above statement, such as if Union or Member States law is modified and/ or require the controller to process personal data. For example, processing data to detect fraud that was previously based on legitimate interests could become based on 'legal obligation' if new statutory rules are introduced forcing firms to do this processing.

Furthermore, the sentence above seems to contradict paragraph 4 of page 22, which states that "*any change in the lawful basis for processing must be notified to a data subject*". Given that there are situations in which the basis for processing may legitimately need to change, we recommend clarifying this point in the Guidelines.

Specific areas of concern in the GDPR (page 23)

Data subject's rights (page 29)

In this part, the Guidelines state that "*[a]t the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome*" (second paragraph, page 29). Although clarifications are welcome, we would suggest deleting the second part of the sentence as it troubles the message and may provide the wrong impression, and confuse, data subjects.

In addition, in the paragraph below, the Guidelines read "*Articles 16 to 20 of the GDPR indicate that when data processing is based on consent, data subjects have the right to erasure, the right to be forgotten when consent has been withdrawn and the rights to restriction, rectification and access*". We would suggest deleting this paragraph as it does not add any information. Furthermore, there seems to be some inaccuracies, with these rights applying much more broadly than just when consent is relied upon.

In addition, it should be kept in mind that the right to rectification only applies to inaccurate or incomplete data. Indeed, the GDPR states in Article 16 that the "*[t]he data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement*". Furthermore, the right of access is mentioned in Article 15 of the GDPR and not in "*Articles 16 to 20*".

EBF suggestion for amendment:

WP29 Guidelines, page 29:

"7.3. Data subject's rights
*If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent****, although the right to withdraw consent at any time may provide a similar outcome****.*

Articles 16 to 20 of the GDPR indicate that when data processing is based on consent, data subjects have the right to erasure, the right to be forgotten when consent has been withdrawn and the rights to restriction, rectification and access."

Consent obtained under Directive 95/46/EC (page 29)

The WP29 states that "*as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted*" (page 30, paragraph 3). Further elaboration would be welcome on that point; particularly on the information which can be excluded.

Under Recital 171 of the GDPR, "*[w]here processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation*". Therefore, we would like to stress that a lack of information about the right to withdraw consent is not an additional condition for the continuity of consent given before May 2018.

Separately, further clarification would be welcome on the following paragraph: *"[i]f a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must assess whether the processing may be based on a different lawful basis, taking into account the conditions set by the GDPR. However, this is a one-off situation as controllers are moving from applying the Directive to applying the GDPR. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing*" (page 30, last paragraph).

Consent is based on freely given consent under legislation that allowed processing under consent. For instance, in some Member States, processing under tacit consent (recognised for example by the Spanish legislation) is lawful until 25 May 2018. From this date, the controller must consider whether consent can be covered by/included in any of the legitimation bases allowed by the GDPR. Among them, for example, the legitimate interest would be a legal alternative that should not be conditioned by what has been done by the controller, according to previous regulation, provided that the requirements of article 6.1 (f) of the GDPR are met, and, the duty to inform the data subject in accordance with Article 13 of the GDPR is accomplished.

However, in the transcribed paragraph, the Guidelines are confusing as they read "*[u]nder the GDPR, it is not possible to swap between one lawful basis and another*". It may be understood that if the basis of legitimacy initially applied (according to an earlier rule) was consent, it is no longer possible to recognize the concurrence of another legally recognized basis in the new regulation, which, moreover, has no retroactive effect.

We believe that this fact would be preventing controllers from recognizing the different legitimation bases accepted by the GDPR. Consequently, a re-drafting of this paragraph would be welcome.

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