28 November 2017
EBF_029539

EUROPEAN BANKING FEDERATION'S COMMENTS ON THE ARTICLE 29 WORKING PARTY GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING – WP251

The European Banking Federation (EBF) appreciates the willingness of the Article 29 Data Protection Working Party (hereafter 'WP29') to offer clarity on automated individual decision-making and profiling. In the EBF's views, it is important to clarify that profiling activities should not necessarily be perceived as having a negative impact on customers. More generally, as far as the banking sector is concerned, profiling is a technique used to provide products and services tailored to customer's needs, facilitate creditworthiness assessment to ensure responsible lending and more importantly to help combating financial crimes in a constantly evolving digital environment where banks are on the front line and where consumers' trust is key.

The approach of the WP29 should reflect the initial approach of the General Data Protection Regulation (GDPR) which aims at providing appropriate and easily understandable information to the data subjects on the use of profiling and automated decision-making with sufficient safeguards against any abuses of direct marketing, according to the existing consumer protection, marketing legislation.

EBF key points:

- **Automated decision-making can be beneficial to individuals and society:** It is important to keep in mind that human decisions are often biased and automated decision-making can therefore help make fairer and more accurate decisions. As stated by the WP29 in its guidelines, automated decision-making can "potentially allow for greater consistency or fairness" or reduce "the risk of customers failing to meet payments for goods or services". We believe this point should also be stressed in the introduction to the guidelines and should be reflected in the interpretation and implementation of the automated decision-making regulatory framework.

  It is important that the profiling and automated decision-making regulatory framework as a whole puts in place appropriate safeguards without blocking the legitimate and socially beneficial uses of these techniques.

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

- **Focus on the "right not to be subject to automated decision-making" in line with the GDPR instead of full prohibition:** The EBF fully supports the objectives of the GDPR to increase transparency around personal data processing and to give data subjects more control over their data. However, the WP29's interpretation of Article 22(1) as a full prohibition is going further than what is prescribed by the GDPR. Instead of using the word 'prohibit' (which the GPDR uses in other articles for instance; see Article 9(1) on the 'processing of special categories of data'), Article 22(1) grants data subjects the right not to be subject to a decision based solely on automated processing of personal data. We believe that the guidelines should be better aligned with the intent of the GDPR and ensure that citizens and data subjects can fully benefit from the rights granted to them by the GDPR.

- **Protect consumers and ensure compliance with existing legal and supervisory requirements**: In financial services, profiling may be used among other things with the view to protect consumers and comply with regulatory/supervisory requirements imposed on the banking sector, such as the Anti-Money Laundering Directive (AMLD) to detect and prevent fraud, terrorism financing or other criminal activity; the Markets in Financial Instruments Directive (MiFID); the Consumer Credit Directive (CCD) or the Mortgage Credit Directive (MCD) with the aim to ensure responsible lending and that individuals do not become over-indebted; it could help the bank to make risk models or to manage the firm's overall financial position. Automated decision making could contribute to achieving these purposes, in accordance with the existing safeguards for the use of direct marketing provided by the current general GDPR and current consumer protection laws.

- **Propose only examples reflecting the general practice of the industry:** Although we appreciate the efforts of the WP29 to provide clarity and reassure stakeholders of their rights, we believe some of the examples provided do not reflect the general practice of the banking sector but represent more marginal examples. This approach could be misleading and could lead data subjects to make false assumptions about their banks. We thus offer changes and amendments to highlight more effectively the potential (and, in many cases, already existing) benefits of automated decision-making and profiling in relation to the financial industry.

- **Importance to ensure consistency between the approach undertaken by the WP29 and the existing EU/national legislation.** In practice, financial services' firms use automated processes to comply effectively and efficiently with high level obligations and guidelines set by financial services regulators/supervisors, including, as mentioned above, obligations on responsible lending and prevention of financial crimes. The Guidelines should clarify that uses of automated decision-making for compliance with rules and guidance set by a

regulatory authority are considered to be 'authorised'. It is important to ensure full consistency with the approach adopted by other regulatory/supervisory bodies, authorities or agencies. In addition, in our view, the approach of the WP29 should be strictly limited to the "protection of persons with regard to the processing of personal data in the Community"[1], to ensure legal certainty and avoid overlaps with existing legislation, for example consumer protection laws, competition law, unfair commercial practices or misleading and comparative advertising directives. Otherwise, it would inevitably create confusion between the roles of the Data Protection Authorities and other authorities.

[1] *Rules of procedure of the Article 29 WP: http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf*

EBF response:

Chapter I of the WP 29 Guidelines - Introduction (page 5)

In its introduction, the WP29 states that "*Profiling can perpetuate existing stereotypes and social segregation"*. The EBF finds this statement disproportionate. Human decisions are often biased and automated decision-making can therefore help make fairer and more accurate decisions. Stigmatisation and limitation of freedom would result from many other factors and not only from the one attributed to profiling.

In addition, as stated by the WP29 in its guidelines, automated decision-making can "*potentially allow for greater consistency or fairness*" or reduce "*the risk of customers failing to meet payments for goods or services*". This point should also be stressed in the introduction to the guidelines and should be a point of reference for the interpretation and design of the automated decision-making framework.

We would thus suggest the following changes:

EBF Suggestion for amendment:

*Profiling**, whether by automated decision-making or through human decision**, can**, in conjunction with other factors,** lead to a perpetuation of existing stereotypes and social segregation. It **~~can~~ could** also lock a person into a specific category and restrict them to their suggested preferences. This **~~can~~ could** undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. It **~~can~~ could** lead to inaccurate predictions, denial of services and goods and unjustified discrimination in some cases.*

Chapter II of the WP 29 Guidelines - Definitions (Page 6-9)

Paragraph A. Profiling

(See page 6 of the WP29 guidelines)

The EBF supports the premise that, in general, decisions should not just be based on certain characteristics. However, in certain contexts this can be appropriate, in the banking sector this is particularly the case in relation to age. The paragraph below (page 7 of the WP29 guidelines) seems to indicate that every decision based on age falls within the definition of profiling. This might be the case, but there can be entirely legitimate reasons why age is an important factor as certain legal implications are always connected to it. For instance, some goods and services are not allowed under a certain age (*e.g.* minimum age to obtain a credit card) and there exists a minimum age foreseen by law to be allowed certain contracts or products (*e.g.* certain pension products or insurance policies).

Another example would be a bank that has a commercial policy to offer free debit card or account to people within a certain age band (*e.g.* young adults); to determine who is eligible for such an offer, the list of clients needs to be sorted by date of birth. A set of clients will be eligible, another set will not. It cannot be argued that this leads to discrimination or to any other unfair disadvantage to a particular client.

In addition, we propose the below amendments in order to better align the Guidelines with the GDPR. Otherwise, classifying minors from other data subjects would be considered profiling. Such automated processing of data has existed for a long time for the above-mentioned reasons and is intended to protect the consumer and the data subject. Moreover, even if this kind of profiling is based on legitimate interest, it would imply (according to the Annex 1 of the guidelines) informing the data subject in line with the transparency principle. However, providing information about that kind of classification could lead to an increase of the information given and overloading the consumers with too many information.

EBF Suggestion for amendment:

The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals. Therefore simply assessing or classifying individuals based on characteristics such as their age, sex, and height ***with a predictive purpose*** *could be considered profiling~~, regardless of any predictive purpose~~.*

Paragraph B. Automated decision-making

(See page 7 of the WP29 guidelines)

We would welcome clarity in the Guidelines concerning the expected role of the individual in the automated decision process. On page 7, automated decision-making is defined as "*the ability to make decisions by technological means without human involvement*". From this statement, one could infer that decisions in which human involvement occurs would not qualify as being automated. However, on page 10, the WP29 states that "*to qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture*". The proposed definitions on page 7 and 10 seem to expect different levels of human involvement, thus bringing ambiguity and uncertainty as to the expected role of the individual.

In addition, we would like to point out that this explanation of what automated decision-making is, creates confusion. Defining automated decision-making by referring to the lack of human involvement seems to differ from what is included in the GDPR. Article 22 GDPR refers to 'human intervention' not as an element of the definition of automated decision but as a right that individuals can invoke when decision-making solely based on automated means takes place. It is one of the guarantees to ensure fairness. This right does not imply the obligation that human intervention must be available at all times.

According to the GDPR, a data subject has the "*right to obtain human intervention*" if and when he or she is subject to a decision based solely on automated processing that produces legal effect or significantly affects him or her.

We would also welcome examples of automated decisions made without profiling. As the WP29 states that classifying people on their age is profiling, every automated decision will then be considered as "based on profiling". However, the WP29 also states that automated decision can be made without profiling. Thus, clarification would be welcome.

Paragraph C. How the GDPR addresses the concepts

(See page 8 of the WP29 guidelines)

The EBF fully supports the objectives of the GDPR to increase transparency around personal data processing and to give data subjects more control over their data. However, as mentioned in our key messages, the WP29's interpretation of Article 22(1) as a full prohibition is going further than what is prescribed by the GDPR. Instead of using the word 'prohibit' (which the GPDR uses in other articles; see Article 9(1) on the 'processing of special categories of data'), Article 22(1) grants data subjects the right not to be subject to purely automated decision-making.

Therefore, the most logical interpretation of Article 22 is that it gives data subjects the right to opt-out from profiling and that automated decision-making can take place if the data subject has consented to it, or when necessary in the context of an agreement, or if there is local legislation that provides specifically for it. To the extent the data controller relies on 'consent' and 'agreement', the data subject has additional rights, such as the right to obtain human intervention, express his or her point of view or contest the decision. Please see more details in the "exceptions to the prohibition" part of our response.

We are thus offering below in our response amendments to better align the Guidelines with the intent of the GDPR and ensure that citizens and data subjects can fully benefit from the rights granted to them by the Regulation. Additionally, we suggest deleting the following sentence "A general prohibition on this type of processing exists to reflect the potentially adverse effect on individuals"

A number of other amendments would be needed throughout the Guidelines to clarify that the GDPR grants data subjects the right not to be subject to purely automated decision-making.

EBF Suggestion for amendment

Chapter III of these guidelines explains the specific provisions that apply to solely automated individual decision-making, including profiling.[2] ~~***A general prohibition on this type of processing exists to reflect the potentially adverse effect on individuals***~~

[2] As defined in Article 22(1) of the GDPR.

Chapter III of the WP 29 Guidelines - Specific provisions on automated decision-making as defined in Article 22 (page 9)

As stated above, Article 22(1) grants data subjects the right not to be subject to purely automated decision-making but does not imply a straightforward prohibition. We would thus like to suggest the following change.

EBF Suggestion for amendment

In summary, Article 22 provides that:

(i) *as a rule, there is a* ***~~prohibition on~~*** ***right of the data subject not to be subject to*** *fully automated individual decision-making, including profiling that has a legal or similarly significant effect;*
(ii) *there are exceptions to the rule;*
(iii) *there should be measures in place to safeguard the data subject's rights and freedoms and legitimate interests.*

Paragraph A. 'Based solely on automated processing'

(See page 7 of the WP29 guidelines)

As mentioned in our comment above, we would welcome clarity in the guidelines concerning the expected role of the individual in the automated decision process. The proposed definitions on page 7 and 10 seem to expect different levels of human involvement, thus bringing ambiguity and uncertainty as to the expected role of the individual.

Paragraph B. 'Legal' or 'similarly significant' effects

(See page 10 of the WP29 guidelines)

- *Paragraph on 'Legal effects'*
  (See page 10 of the WP29 guidelines)

We believe here that the WP29 goes beyond issues related to data protection and data privacy. This part clearly overlaps with existing legislation, notably consumer protection laws, and we believe this would inevitably create confusion between the roles of the DPAs and other authorities.

On the last examples provided by the WP29 ("*automatically disconnected from their mobile phone service for breach of contract because they forgot to pay their bill before going on holiday*" – page 10 of the Guidelines), the EBF would welcome clarification as it is our understanding that it may not be fully coherent with the arguments used (rights recognised within a legal framework or a contract) because there is not a right to not accomplish an obligation established contractually and legitimately between the parties. Moreover, there are other legal instruments which delimit the degree of fault or negligence applicable to the parties in the accomplishment of their obligations. Therefore, although enforcing a contract would have a 'legal effect', the guidelines should recognise that this would come within Article 22 (2)(a), being necessary for a contract.

- *Paragraph on 'Similarly significantly affects him or her'*
  (See page 10 of the WP29 guidelines)

Of course, the question of when a 'similarly significant' effect has to be considered cannot be easily answered, but certain clarity would be welcomed. The definition of a 'similarly significant' effect as an effect that "*must be more than trivial*" (in the third paragraph under this part, page 10) is quite vague, especially as 'trivial' is normally used to express a matter of little or no importance.

The explanation continues stating that "*the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned*" which does not make the situation clearer as there is hardly any situation where there would be no influence on the individual. The ambiguity that needs to be resolved is when this influence is '*significant*'. It should also be clear that such an effect would be negative, as there may be decisions, including based on profiling, which have a positive effect on individuals and which do not fall under the restrictions set out by Article 22(1). In addition, clarification, notably through examples, of the word "*circumstances*" would be welcome.

Examples are useful in principle. However, a more concrete set of examples would be welcome to better understand the WP29 understanding of "*not trivial*" and "*similarly significant*", as the guidance seems to set an extremely low bar for '*significant'*. For example, if a bike rental of two hours is already significant, this suggests a very large range of decisions would be significant given this is likely to be an inexpensive service. Clarity on what defines 'significant' in this case would be welcome as this example could be interpreted as meaning that every access to goods and services is *per se* significant or that it entails every kind of activity of a normal person.

We would suggest deleting the part regarding targeted advertising (page 11). Targeted advertising as such hardly implies a 'significant effect' for the clients of our industry (see our example below). The WP29 should carefully consider the potential for unintended consequences if targeted advertising is to be frequently seen as having '*significant effects*', particularly if Article 22 (1) is to be interpreted as a prohibition. To consider targeted advertising in certain cases as a 'similarly significant effect' is worrisome. There is a risk that particular characteristics that define when targeted advertising has to be considered a '*similarly significant effect'* can be interpreted widely as well.

Without prejudice to our point above, we would welcome clarification on the below paragraph (page 11):
"However it is possible that it may do, depending upon the particular characteristics of the case, including:

- *the intrusiveness of the profiling process;*
- *the expectations and wishes of the individuals concerned;*
- *the way the advert is delivered; or*
- *the particular vulnerabilities of the data subjects targeted."*

We consider the addition of new criteria by the WP29 to be disproportionate and going beyond the provisions set-up by the GDPR. This is especially the case for "*the intrusiveness of the profiling process*" and "*the expectations and wishes of the individuals concerned*". The meaning of these criteria is unclear.

There is a risk that if this threshold is too low, data protection authorities (DPAs) will find themselves regulating advertising standards which go beyond their mandate and could create legal uncertainty and overlap with existing legislation, for example under Directive 2006/114. The specialised regulatory frameworks governing advertising should be relied on in the first instance, with DPAs focusing only on the most significant examples with clear privacy implications. For instance, a bank that wants to promote its mortgages may want to exclude its clients who already have a mortgage with them, and will target the clients with a bank account who do not have a mortgage. This occurs on the basis of profiling. In this situation, the target is: client of the bank with a bank account, without a mortgage at the bank, and who is older than 18. That these persons are targeted with an advertisement for a mortgage will not have a significant impact on them nor will their privacy be disproportionately affected.

In addition, we would also welcome clarity on the meaning of "*particular vulnerabilities of the data subjects targeted*" as this last criterion should only apply insofar as such vulnerabilities are known to the controller.

Regarding the following sentence: "*Automated decision-making that results in differential pricing could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services*", we are of the view that the approach of the WP29 goes beyond the "protection of persons with regard to the processing of personal data in the Community"[3] and could create overlaps with existing legislation, for example consumer protection laws, competition law, unfair commercial practices or misleading and comparative advertising directives. We believe existing consumer protection legislation in the sphere of financial services is adequate and any overlap risks creating inconsistency in the treatment of consumers.

This sentence should be deleted as it would otherwise inevitably create confusion between the roles of the Data Protection Authorities and other authorities.

[3] *Rules of procedure of the Article 29 WP: http://ec.europa.eu/justice/data-protection/article-29/files/rules-art-29_en.pdf*

We agree that fair outcomes are important but consider this is a matter for financial services regulation and anti-discrimination legislation and not (so much) for privacy regulation.

Finally, regarding the example of the credit card company (page 11), we would suggest deleting this example as it is misleading. It seems to imply that this practice happens on a daily basis and that this would be the only criterion to obtain a credit card. In practice, financial institutions take into account many other factors. The risk model required from a regulatory point of view obliges entities to analyse the clients' insolvency risk in what has been defined as responsible lending. This involves an assessment of his or her future capability to make repayments depending on various factors, as observed in respect of other individuals with similar circumstances. Regulators insist in using knowledge and techniques designed to protect consumers from being over-credited. As such, the example above is not accurate.

It needs to be made clear that, though this is an example of 'significant effect', it would be a legitimate use of automated decision-making, provided the firm is transparent with the customer and provides an opportunity to have the decisions reassessed.

In addition, the argument can be made that the example is not relevant as he decision is made in the context of executing a contract, where automated decision-making is allowed. The consumer could then, if he or she decides to do so, request human intervention.

Paragraph C. Exceptions from the prohibition

(See page 12 of the WP29 guidelines)

As mentioned previously, in financial services, profiling may be used among other things with a view to protect customers and comply with EU and national requirements imposed on financial institutions, so as to ensure responsible lending and individuals not becoming over indebted, in order to make risk-models; to manage the firm's overall financial position; and to help detecting and preventing fraud, terrorism financing and other criminal activity. Automated decision-making could contribute to the these purposes. It would be socially detrimental to prevent these positive uses of automated decision-making.

Consequently, firms need clarity and assurance that personal data may continue to be processed using profiling and where (technically and financially) possible - and within the legal boundaries - explore whether automatic decision making could be used for these purposes. Although this processing might be expected by regulators, and recommended in guidance, it is not all based on an explicit legal obligation.

An overly narrow interpretation of the GDPR could considerably limit the ways financial institutions may use data-analytics to:

- detect and prevent fraud, terrorism financing, money laundering and other crimes;
- executing credit checks to ensure product suitability and customers not becoming over-indebted;

- ensure marketing is appropriate, such as avoiding credit card marketing to customers at risk of over indebtedness;
- protect the financial robustness of the firm by ensuring that loans issues will not put the firm in breach of prudential requirements.

The collection of personal data and its analysis is necessary for profiling for risk management, creditworthiness assessment purposes and financial crime prevention - for example for fine-tuning the parameters used in fraud monitoring systems to improve their ability to detect and prevent related fraud, as requested by financial services requirements. These procedures are widely recognised to be the most effective and fair (if not the only possible) way of assimilating data in order to make responsible financial decisions. Actually, their use can derive from legal requirements in various EU and national laws such as the Anti-Money Laundering Directive (AMLD)[4] which imposes a customer due diligence and Know Your Customers requirements as well as the Markets in Financial Instruments Directive (MiFID)[5], the Consumer Credit Directive[6] or the Mortgage Credit Directive[7]. This processing is frequently based on the controller's 'legitimate interest' according to the GDPR.

---

[4] Article 13(1)(a) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC provides that Customer due diligence measures shall comprise: *identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.*

[5] Article 13(5) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC provides that *(…) An investment firm shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems.*

[6] *Article 8 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April on credit agreements for consumers and repealing Council Directive 87/102/EEC provides that Member States shall ensure that, before the conclusion of the credit agreement, the creditor assesses the consumer's creditworthiness on the basis of sufficient information, where appropriate obtained from the consumer and, where necessary, on the basis of a consultation of the relevant database.*

[7] Article 18 of Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 concerning the obligation to assess the creditworthiness of the consumer provides:

1. Member States shall ensure that, before concluding a credit agreement, the creditor makes a thorough assessment of the consumer's creditworthiness. That assessment shall take appropriate account of factors relevant to verifying the prospect of the consumer to meet his obligations under the credit agreement.

2. Member States shall ensure that the procedures and information on which the assessment is based are established, documented and maintained.

[…] 5. Member States shall ensure that:

(a) the creditor only makes the credit available to the consumer where the result of the creditworthiness assessment indicates that the obligations resulting from the credit agreement are likely to be met in the manner required under that agreement;

If the 'prohibition' is retained as the interpretation by WP29, the guidance therefore needs to accommodate such processing. This should involve:

- recognising that the exemption in Article 22(2)(a) for 'contract' can be interpreted broadly, and not narrowly as with the Article 6 basis for processing;
- automated decision-making for the purposes of compliance with regulatory requirements and guidance is to be considered 'authorised' under Article 22(2)(b). This is especially true in the banking industry where, before entering into a contract or in the processes of entering it, the bank needs to perform a number of checks and balances before a product is awarded (for example, Know Your Customer obligations or observing due-care before allowing a client to be accepted for a given product). Without these checks, individuals cannot become clients. These checks go hand in hand with the conclusion of an agreement in our industry. Without these, it would be irresponsible to enter into an agreement with a customer. Hence, the interpretation of the WP29 is too restrictive here.

◆ *Paragraph For the performance of a contract*
(See page 12 of the WP29 guidelines)

Much of the decision-making outlined in this part might reasonably be thought of as permissible under Article 22 (2)(a), being '*necessary for a contract*'. However, the draft Guidelines states that this needs to be interpreted narrowly, referencing the 2014 guidance on legitimate interests. The guidance from 2014 states (pages 16–17) that '*necessary for contract*' would exclude processing to prevent fraud, pre-contractual credit checks, etc.

We recommend that the final Guidelines make clear that Article 22(2) (a) is not a reference to the 'basis for processing' under Article 6 and can be interpreted more broadly. We note that Article 22(2) uses different language than Article 6. Article 22(2) refers to a 'decision' being necessary for the contract, while Article 6 refers to specific 'processing' being necessary, which is a different and narrower test.

(b)in accordance with Article 10 of Directive 95/46/EC, the creditor informs the consumer in advance that a database is to be consulted;
(c) where the credit application is rejected the creditor informs the consumer without delay of the rejection and, where applicable, that the decision is based on automated processing of data. Where the rejection is based on the result of the database consultation, the creditor shall inform the consumer of the result of such consultation and of the particulars of the database consulted.
6. Member States shall ensure that the consumer's creditworthiness is re-assessed on the basis of updated information before any significant increase in the total amount of credit is granted after the conclusion of the credit agreement unless such additional credit was envisaged and included in the original creditworthiness assessment.
7. This Article shall be without prejudice to Directive 95/46/EC.

- *Paragraph on 'Authorised by Union or Member State law'*
  (See page 12 of the WP29 guidelines)

  Similarly, the processing outlined in this part might be expected to be covered by Article 22 (2)(b). However, the draft Guidelines do not explain how this provision should be interpreted.

  Where firms have an obligation in statute to use automated decision-making, this would presumably be within Article 22 (2)(b). However, in practice, financial services' firms use automated processes to comply effectively and efficiently with high level obligations and guidelines set by financial services' regulators, including, as mentioned above, obligations to lend responsibly and to prevent financial crime.

  The Guidelines should clarify that uses of automated decision-making for compliance with rules and guidance set by a regulatory authority are considered to be 'authorised'. It is important to ensure full consistency with other regulatory bodies.

- *Paragraph on Explicit consent*
  (See page 13 of the WP29 guidelines)

  By considering that 'explicit consent' is not defined in the GDPR but that the consent must be specifically confirmed by an express statement rather than some other affirmative action, we believe the WP29 goes further than the affirmative action required by the GDPR. We would thus suggest deleting this sentence.

  We would also like to point out that financial institutions could not rely on consent for the processing operations described in "C. Exceptions from the prohibition" as these are not optional additional services. According to the different requirements with which banks have to comply, banks could not accept a customer withdrawing consent to AML checks, fraud monitoring, etc. which are acknowledge as legitimate interest as per Recital 47 of the GDPR.

EBF suggestion for amendment:

~~***'Explicit consent' is not defined in the GDPR but suggests that the consent must be specifically confirmed by an express statement rather than some other affirmative action.***~~

Paragraph D. Rights of the Data Subject

(See page 13 of the WP29 guidelines)

- *Paragraph 1 - Article 13 (2) (f) and 14 (2) (g) – right to be informed*
  (See page 13 of the WP29 guidelines)

The EBF would welcome clarifications regarding the right to information in respect of automated individual decision-making and profiling. We are however concerned with the sentence "*This means ensuring that information about profiling is not only easily accessible for a data subject but* ***that it is brought to their attention***" (page 13). This extra requirement is neither in the body of the GDPR nor in the Recitals. Ensuring adequate information can be obtained through websites (or other means) which data subjects can consult, if and when they want, should be enough.

We would be interested to know what kind of information a data controller needs to give the data subject regarding the process or processes in these cases. In some cases, it is important to note that the data process used may have elements related to "business secrecy" (*e.g.* credit scoring models). The EBF is also concerned about the word-choice in the following sentence "*tell the data subject that they are engaging in this type of activity*" (page 13). The use of the word "tell" creates confusion and certainty on how it should be interpreted would be welcome.

In addition, we welcome the aspiration of the WP29 to provide best practices and concrete examples. However, we believe it to be important not to exceed what the GDPR requires as seems to be the case with the following sentence: "*It is good practice to provide the above information whether or not the processing falls within the narrow Article 22(1) definition*".

- *Paragraph 2 - Article 22 (1) – right not to be subject to a decision based solely on automated decision-making:*
  (See page 15 of the WP29 guidelines)

The EBF fully supports the objectives of the GDPR to increase transparency around personal data processing and to give data subjects more control over their data. However, the WP29's interpretation of Article 22(1) as a full prohibition is going further than what is prescribed by the GDPR. Instead of using the word 'prohibit' (which the GPDR uses in other articles for instance; see Article 9(1) on the 'processing of special categories of data'), Article 22(1) grants data subjects the right not to be subject to a decision based solely on automated processing of personal data. We believe that the guidelines should be better aligned with the intent of the GDPR and that ensure citizens and data subjects can fully benefit from the rights granted to them by the GDPR.

We therefore suggest replacing the wording "*acts as a prohibition*" by "*provides a right to the data subject not to be subject to*" (please see our suggestion for amendment below).

On human intervention, the WP29 states that "[h]*uman intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject*" (last paragraph, page 15). We would welcome clarification on this point. The place where the balance between the subject's right to ask for the human intervention, and the exceptions applicable to the financial sector would be struck, is not clear. In particular, regarding the obligation of "responsible lending" and the internal procedures to improve the efficiency of the granting of credits and loans which are inherent in the act of entering a contractual relationship.

EBF suggestion for amendment

As explained earlier in this chapter, Article 22(1) ***provides a right to the data subject not to be subject to*** ~~***acts as a prohibition on***~~ *solely automated individual decision-making, including profiling with legal or similarly significant effects. Instead of the data subject having to actively object to the processing, the controller can only carry out the processing if one of the three exceptions covered in Article 22(2) applies.*

Chapter IV. of the WP 29 guidelines - General provisions on profiling and automated decision-making (page 17)

Paragraph A. Data protection principles

(See page 17 of the WP29 guidelines)

- *Paragraph 1 - Article 5(1) (a) – Lawful, fair and transparent*
  (See page 17 of the WP29 guidelines)

The WP29 states that "*For data collected directly from the data subject this should be provided at the time of collection (Article 13); for indirectly obtained data the information should be provided within the timescales set out in Article 14(3)".* The EBF would welcome clarification on the meaning of "*indirectly obtained data*" (in the fourth paragraph of the part, page 17). Article 14 of the GDPR refers to data that has not been obtained from the data subject, thus from a third party. As the guidelines on transparency have not yet been published, clarity in this part would be useful to understand more clearly what is expected of the controller.

In addition, the EBF would welcome clarification on the example of insurers offering insurance rates and services based on an individual's driving behaviour. In this example, it is unclear if there is a lawful basis and if so, which lawful basis could be used. The final Guidelines should clarify that this activity would be covered by Article 22 (2)(a).

We would suggest that the WP29 delete the sentence "*Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit*

or insurance, or targeting them with excessively risky or costly financial products". Indeed, it is important to recall that in view of the problems brought to light during the financial crisis, specific requirements are imposed on the banking sector, notably, by the Mortgage Credit Directive in order to prevent irresponsible lending and borrowing. Banks have to conduct a thorough assessment of creditworthiness which focuses on the consumer's ability to meet their obligations under the credit agreement and have therefore a legal duty to deny access to credit to people who cannot reimburse it. Recent legislation adopted in the last few years such as the Key information documents for packaged retail and insurance-based investment products (PRIIPs), the Insurance Distribution Directive (IDD) or the Directive on markets in financial instruments (MiFID 2) also impose obligations on the banking sector to sell a product or service which meets the needs of the client. MiFID 2 clearly states for example that investment firms should act in accordance with the best interests of their clients when providing them with investment services. These firms should safeguard their clients' assets or ensure the products they intend to launch are designed to meet the needs of clients. Investors will also be provided with increased information on products and services offered or sold to them. This type of "profiling" is not unfair nor does it create discrimination.

It is also important to recall that several consumer protection principles, including the Unfair Commercial Practices Directive (UCPD)[8], and the related European Commission's guidance, aim at preventing the behaviour described in the example. For financial services, Member States have even put in place national rules that provide consumers with stricter safeguards which add to and complement those laid down in the UCPD. The following amendment should therefore be supported.

EBF suggestion for amendment:

~~***Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products.***~~

In addition, the examples related to a data broker selling consumer profiles to financial companies without consumer permission or knowledge of the underlying data or referring negatively to payday loans, casts a very negative light on the European banking sector. This example is, in our view, misleading in making the reader believe that this practice occurs frequently in Europe when this is not the case. It mostly refers to a practice done outside the European Union or only in very specific countries. We therefore suggest the deletion of this example.

[8] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council

EBF suggestion for amendment

~~***Example***~~

~~***A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products).***~~

Paragraph B. Lawful bases for processing

(See page 20-21 of the WP29 guidelines)

- *Paragraph 1 - Article 6(1) (a) – consent*
  (See page 20 of the WP29 guidelines)

  The WP29 Guidelines states that *"Profiling can be opaque. Often it relies upon data that is derived or inferred from other data, rather than data directly provided by the data subject"* Regarding the use of the word "*opaque*", we believe that such situation is prevented by Article 13 and Article 14 of the GDPR (Information to be provided where personal data are collected from the data subject and Information to be provided where personal data have not been obtained from the data subject). However, as noted above in our paper, in some cases, it is important to note that due to specific requirements imposed on the banking sector, some elements used in the data process may relate for example to fraud prevention or "business secrecy" and, as such, cannot be disclosed. We believe that the categories and/ or the nature of the information used are enough to provide clarity for data subjects. We would therefore suggest the deletion of the reference to 'opaque'.

  We would also welcome clarifications on the following sentence which reads: "*Often it [profiling] relies upon data that is derived or inferred from other data, rather than data directly provided by the data subject*". As mentioned in the above paragraph, data subjects have to be given a substantive amount of information regarding data that have not been obtained by them. We would thus welcome further explanation on what the WP29 is trying to explain with these sentences.

- *Paragraph 2 - Article 6(1) (b) – necessary for the performance of a contract*
  (See page 20 of the WP29 guidelines)

  The WP29 Guidelines refers to an example on the practice of online retailers and the fact that the online retailer builds a profile of the users' tastes and lifestyle choices based on their website visits.

Provided that this information is limited and not too intrusive and that the controller states appropriately how this information will be used and offers the right to object, it can be argued that in this case the profiling is carried on according to the legitimate interest of the controller as per Article 6(1)(f) of the GDPR and it seems to be lawful (also when considering Article 21(2) GDPR). Of course, if this information is tracked and recorded through cookies, and is not downloaded based on the information the client might have provided in a questionnaire or that is derived from the use that is made of the service, it will be likely that consent is first sought for placing the cookies which will enable the collecting of the information.

The Guidelines should make clear that 'legitimate' interests' could still be a valid basis for processing. Please see our comments above in our response.

- *Paragraph 6 - Article 6(1) (f) – necessary for the legitimate interests pursued by the controller or by a third party*
  (See page 21 of the WP29 guidelines)

We would appreciate if the WP29 would explain the content of the four parameters indicated on page 21, providing some practical and realistic examples. We would also welcome if the WP29 could (i) specify whether all or few of the said parameters will apply and whether some of them will be considered prevalent and (ii) confirm that they apply only to processing carried out according to Article 6 (1)(f).

Paragraph D. Rights of the Data Subject

(See page 23 of the WP29 guidelines)

We would suggest deleting the following sentence "*The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed"* (last sentence of the fourth paragraph of the example, page 23). As mentioned above in our comments, notably on the part dedicated to article 6 (1)(a) on consent, we believe that keeping this sentence in the guidelines could have adverse effects on some processing required for anti-money laundering and terrorism financing purposes. Some of the categorisations made should remain confidential.

EBF suggestion for amendment:

Example

(…)

~~**The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed.**~~

- *Paragraph 4 - Article 21 – right to object:*
  (See page 23 of the WP29 guidelines)

We notice a number of inconsistencies in this part of the Guidelines and an interpretation that goes beyond the risk-based nature of the GDPR.

The WP 29 guidelines state that "*Once the data subject exercises this right, the controller must interrupt (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests or rights and freedoms of the data subject. The controller may also have to erase the relevant personal data*". This paragraph seems to imply an automatic obligation to interrupt the profiling process if the data subject exercises the right to object. This is not our legal interpretation. When the data subject exercises the right to object, the data subject may ask for the blocking of the data. The GDPR does not provide for this automatic triggering of the restriction of processing just because an objection has been made under Article 21. The right to object and the right to restrict are two separate rights and they are not contingent one upon the other as this paragraph would suggest. When the data subject asks to object, the controller needs to consider the objection presented but it is not automatically obliged to discontinue the processing of data.

It is also, in our opinion, misleading to state that the controller may have to erase the relevant personal data when an objection has been filed. Erasing data may have to take place only if the data controller does not need the data for another reason (ground or purpose); for example, after the legal mandatory retention periods have lapsed and the data is not necessary for statistics or research. Article 17 of the GDPR is quite clear: there are rather important and relevant exceptions to the right to be forgotten. These rather exceptional situations described in Article 17 of the GDPR, according to which the right to be forgotten may not be honoured, are frequent in the case of a highly regulated industry like the banking sector. Also in this case, when a data subject exercises the right to object, this does not automatically trigger the need to erase the data. The exceptions of Article 17 may still apply. This paragraph in the Guidelines is misleading for data subjects and should therefore be deleted.

We believe the WP29 goes further and gives an interpretation of what is considered 'compelling legitimate grounds' that goes beyond what the European legislator meant.

There are situations in the banking industry and in the way banking services are provided that require processing personal data based on the legitimate interests of the controller. When banks rely on this ground, it means that a balance of interest has been carried out. There are many examples of processing of data that are necessary in the context of how the bank organises itself and its business that have a minimal impact on the privacy of individuals. For example, clients may be segmented between "retail" and "private banking" according to certain characteristics they have. The types of products and services that are provided to retail clients and those that are offered to private banking are different. This type of profiling: a client falls into the 'bucket' retail or into the 'bucket' "private banking" constitutes a processing of personal data. In this situation, the industry understands that the client has a right to object. The client is free to exercise this right.

If a bank is confronted with such an objection, the bank will consider it and adequately and respectfully let the client know that it will not honour the objection presented to this processing. If clients were to object to this, and banks were forced to honour such objections, this would have a profound and disruptive effect in the way it conducts its business; which has never been the purpose of this provision.

EBF suggestion for amendment

~~***Once the data subject exercises this right, the controller must interrupt (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests or rights and freedoms of the data subject. The controller may also have to erase the relevant personal data.***~~

In addition, we would welcome further clarification on this part of the Guidelines. We fail to understand why the right to object also applies when the legal ground for processing is either "*necessary for the performance of a contract*", "*consent*" or a "*legal obligation*". As far as we understand, the right to object applies when the legitimate basis for the processing is the "*legitimate interest*" of the controller.

The WP29 asserts that the rights of data subjects (including the right to object), listed in Chapter IV, Section D of the guidelines, are applicable on both profiling and automated decision-making (see page 17 and note 32 on page 22 of the guidelines). However, if the WP29 considers and reads the provision of Article 22 GDPR as a straightforward prohibition, the right to object would not be applicable to automated processing (including profiling).

The WP29 guidelines also refer to specific elements that the data controller would need to prove, including "*the objective is critical for the organisation*". We believe that the wording "critical" is too restrictive and should be replaced by "important"

EBF Suggestion for amendment

The controller would also need to prove that:

- the impact on data subjects is limited to the minimum necessary to meet the particular objective (i.e. the profiling is the least intrusive way to achieve this); and
- the objective is ~~**critical**~~ **important** for the organisation.

Good practice recommendations in Annex 1:

(See page 28 of the WP29 guidelines)

As a general comment, we would like to stress that, under Article 22 of the GDPR, the rights granted are different whether we talk about profiling or about automated decision-making. We believe a clear distinction should be made in the good practice recommendations.

In addition, we offer you the following comments and amendments:

- ***On the right to have information:***

  - We believe the good practice described below by the WP29 goes beyond the scope of the GDPR. We understand the need to provide information about the logic involved; however, it should be left up to the banks how to provide information, and which kind, to make sense to the data subject. In addition, we suggest waiting until the full implementation of the GDPR to see how the right to have information will be best applied and fully empower data subjects.

  - We consider that the level of information to be provided is too extensive and that it runs in contradiction to Article 12 (1) which asks for information to be provided in a concise manner. We have thus proposed the below amendment. Moreover, we believe there is a contradiction between the fact that documents providing information to data subjects have to be simple and easy to understand and the length of requirements and the good practice here. Controllers should be reassured that they will be evaluated in their customer communication on their effort to communicate transparently and effectively to a mass audience.

EBF suggestion for amendment

Right to have information:

Controllers may wish to consider:

- *layered notices, where data subjects are informed about the processing of their data on a step by step basis. This type of approach can work by providing the key privacy information in a short notice, with links to expand each section to its full version, and a just in time notification at the point where the data is collected;*
- *visualisation and interactive techniques to aid algorithmic transparency[46];*
- *standardised icons[47] to inform individuals about profiling and automated decision-making, for example:*
  - *The organisation shares their personal data with other organisations;*
  - *Details of the other organisations with whom their personal data is shared;*

- *Whether this/these organisation(s) is/are using their personal data to profile them;*
- *Whether the profile is being used to make decisions about them.*

*Meaningful information about the logic involved will in most cases require controllers to provide details**. ~~such as:~~***

- ***~~the information used in the automated decision-making process, including the categories of data used in a profile;~~***
- ***~~the source of that information;~~***
- ***~~how any profile used in the automated decision-making process is built, including any statistics used in the analysis;~~***
- ***~~why this profile is relevant to the automated decision-making process; and~~***
- ***~~how it is used for a decision concerning the data subject.~~***

- ***On consent as a basis for processing***

  - On the good practice regarding "*consent as a basis for processing*" (page 29), we would like to stress the importance of taking into account the possibility to create "consent fatigue" for consumers and data subjects. An appropriate level of granularity needs to be found that does not lead the consumer to be nudged and bothered constantly.

- ***On the right of access***

  - Considering that an algorithm's parameters will be as complex for the data subject as the algorithm itself we suggest referring also to "parameters".

  - In addition, we understand the right of access is a right of the individual, not of "an expert" or third party. The right of access does not go as far as to have to disclose this information to be able to "help" experts. In order to reflect fully the GDPR requirements, we would suggest the deletion of the following sentence *"although the latter should also be provided if this is necessary to allow experts to further verify how the decision–making process works".*

EBF suggestion for amendment

Right of access:
Information about the categories of data that have been or will be used in the profiling or decision-making process and why these are considered pertinent will generally be more relevant than providing a complex mathematical explanation about how algorithms, ***their parameters*** *or machine learning work**~~, although the latter should also be provided if this is necessary to allow experts to further verify how the decision-making process works~~**.*

Controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it.

- ***On appropriate safeguards***

  - Article 22 of the GDPR does not focus on profiling but on a decision based solely on automated means, including profiling, which is stricter. We thus propose to align the first part of the example with the text of the GDPR.

  - In addition, provision should be made for the fact that probabilistic algorithms inherently lead to a fraction of false negatives and false positives outcome. What really matters is that the models are statistically validated to ensure they work as intended.

EBF suggestion for amendment

Appropriate safeguards:
The following list, though not exhaustive, provides some good practice suggestions for controllers to consider ***when solely automated decision-making based on*** *profiling* ***has a legal or similar significant effect****:*

- *regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise;*
- *algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended* ***and that they are statistically validated~~, and not producing discriminatory, erroneous or unjustified results~~****;*
- *specific measures for data minimisation to incorporate clear retention periods for profiles and for any personal data used when creating or applying the profiles;*
- *using anonymisation or pseudonymisation techniques in the context of profiling;*
- *ways to allow the data subject to express his or her point of view and contest the decision; and,*
- *a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries .*

Controllers can also explore options such as:

- *certification mechanisms for processing operations;*
- *codes of conduct for auditing processes involving machine learning;*
- *ethical review boards to assess the potential harms and benefits to society of particular applications for profiling.*

Contacts:

Noémie PAPP
Head of Digital & Retail
n.papp@ebf.eu

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

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:

Noémie PAPP
Head of Digital & Retail
n.papp@ebf.eu

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