Sent by email to:
JUST-ARTICLE29WP-SEC@ec.europa.eu
presidenceg29@cnil.fr

28 November 2017

Response to draft *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*

Dear Sir or Madam,

Thank you for the opportunity to respond to the draft Guidelines on automated decision-making and profiling. This is a joint response from UK Finance and the Association for Financial Markets in Europe (AFME).[1]

Our annexed response focuses on the impact of Article 22, as interpreted by the draft Guidelines, on important uses of automated decision-making in the financial services sector designed to help achieve compliance with regulatory obligations and guidance.

Our concerns stem from the combination of:

- The interpretation of Article 22(1) as a prohibition.
- The wide scope of 'significant effect'.
- The narrow interpretation of the exemptions in Article 22(2).

These components together risk inhibiting or preventing the use of automated decision-making in the financial services sector. This processing is aimed at protecting customers, preventing crime and achieving other public policy objectives.

We would be happy to discuss further with you and to answer any questions you may have.

Yours faithfully,

Walter McCahon

Policy analyst
UK Finance
T +44 20 3934 1131| M +44 7 725 683263
E walter.mccahon@ukfinance.org.uk

Richard Middleton

Managing Director
AFME
T +44 20 3828 2709 | M +44 7584 583 122
E richard.middleton@afme.eu

[1] AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society. AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is registered on the EU Transparency Register, registration number 65110063986-76.

UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities. The interests of our members' customers are at the heart of our work.

Primary issue: preservation of automated decision-making for beneficial purposes

Our response makes some mention of profiling broadly but is concentrated on the rules governing the use of automated decision-making (ADM) under Article 22.

Appropriate safeguards need to be in place when ADM is used…

Use of ADM and profiling does of course carry with it certain risks. In accordance with the GDPR, the draft Guidelines correctly identify that certain safeguards are required so as to ensure that individuals are treated fairly and that their rights are protected. In particular, measures need to be in place to ensure:

- data subjects understand how ADM is being used
- algorithms function correctly
- individuals have an opportunity to have their case re-examined if they disagree with a decision

These safeguards are in addition to extensive obligations imposed under financial services regulation to ensure that customers are treated fairly and that vulnerable customers are given additional support.

…but ADM can also protect data subjects and help achieve public policy goals…

The introduction to the draft Guidelines correctly observes that ADM can provide efficiency benefits and resource savings, but these are only a small part of the benefits that use of ADM offers. Use of automated decisions helps firms to apply a consistent approach to service provision. This helps avoid unfair outcomes for customers caused by human error or bias.

Furthermore, in the financial services sector ADM is used for a range of purposes that are vital to the financial services sector (the '***core FS purposes***'), including in particular to:

1. Allow real-time decisions on whether to carry out or block transactions due to suspicions that the transaction is fraudulent, or concerns of money laundering, terrorist financing or other criminal activity
2. Decide not to employ a certain individual for a regulated function on the basis of automated screening against a government list covering certain offences and convictions (such as the Disclosure and Barring Service in the UK) in order to comply with regulatory obligations governing employment for key roles in financial services
3. Decide whether to accept or reject a product application due to the (potential) customer's creditworthiness or affordability concerns
4. Decide to reduce a customer's credit card or overdraft limit in order to ensure he/she does not become over indebted and experience financial hardship
5. Decide whether to make a loan to an individual, on the basis of the impact of that loan on the overall capital position of the firm in order to protect its overall financial robustness in compliance with prudential regulatory obligations.

ADM is used in these contexts in order to protect customers and meet other important public policy objectives. These are also in order to satisfy the expectations and guidance from financial services regulatory authorities.

It is not practical or socially beneficial for these protections to operate without ADM. To take some examples:

- There are billions of transactions processed every year. It is not possible for fraud detection, AML screening, assessments of overall customer indebtedness, etc, to be conducted without ADM.
- Similarly, firms receive large numbers of applications for relatively low value loans and overdraft facilities. Where adequate credit data is available, automated credit checks provide an efficient means to make decisions in the necessary volumes while applying consistent and independent criteria to all applicants and ensuring lending meets regulators' responsible lending expectations.

The current draft Guidelines may be interpreted as <u>preventing</u> these beneficial uses

As noted above, we agree with the importance of having appropriate safeguards in place. However, WP29 should make sure that the Guidelines do not inadvertently *prevent* the use of ADM for regulatory and other socially beneficial purposes.

It may be that WP29 does not intend for all of the examples above to be caught under Article 22. However, as outlined in more detail below:

- The Guidelines as presently drafted do suggest that all of these activities could potentially be subject to Article 22, given the low threshold for 'significant effect'.
- The Guidelines as presently drafted apply the exemptions in Article 22(2) narrowly, which might be interpreted as preventing these core FS uses of ADM.

These points, combined with the interpretation of Article 22(1) as a prohibition, create a risk that the use of ADM for the ***core FS purposes*** will indeed be caught by Article 22 and prevented.

Applying Article 22(1) as a prohibition is a big change

Article 22(1) is difficult to interpret; we note that there are different views from law firms online as to whether it amounts to a *prohibition* on (certain) ADM, or whether it is instead a right to *request* a human decision.

A move to a prohibition is a significant change compared to the regime under the Data Protection Directive as it is applied in some Member States, which operate instead on the basis of a right to require a human decision on request.

WP29 should consider carefully whether a prohibition is the correct interpretation of Article 22(1) and whether this is the best way to protect data subjects in the emerging data economy.

If there is a move to a prohibition, unintended consequences are likely. If this interpretation is retained, WP29 should take care to ensure that these are minimised. In particular, it is important to make sure that beneficial uses of ADM are able to continue post-May 2018. This will require appropriate application of the exemptions in Article 22(2). **If the interpretation of the exemptions is too narrow, this will risk undermining these ADM uses to the detriment of customers and other individuals.**

We note that some of the ***core FS purposes*** are referenced in the draft Guidelines, suggesting that the WP29 sees them as legitimate. However, at present the Guidelines as currently drafted risk having the effect that these uses of ADM would in practice not be able to continue.

Recommendation: WP29 should consider carefully whether Article 22(1) should be interpreted as a prohibition.

The exemptions in Article 22(2) need to be interpreted appropriately

If the interpretation of Article 22(1) as a prohibition is retained, it will be necessary to rely on the exemptions in Article 22(2) in order to continue using ADM for the ***core FS purposes***.

The use of ADM for the ***core FS purposes*** should fall within Article 22(2)(a), but this is unclear under the Guidelines.

Similarly, given that the ***core FS purposes*** reflect the need to comply with guidance and rules imposed by financial services regulators, intuitively the exemption in Article 22(2)(b) should apply, but this is not clear under the Guidelines.

In contrast, Article 22(2)(c) is not a feasible alternative, as a firm could not make ADM for the ***core FS purposes*** optional.

Necessity for contract: Article 22(2) is not a reference to the Article 6 bases for processing and should be interpreted more broadly

Intuitively, the ***core FS purposes*** set out above could be said to be within Article 22(2)(a): "[the decision] is necessary for entering into, or performance of, a contract between the data subject and a data controller". Indeed, this is the view that representatives of more than one Data Protection Authority have given to us and to our members in separate discussions, and it would seem to be an appropriate interpretation to allow core processing of this type.

However, the draft Guidelines take a very narrow view of this exemption and seem to exclude the ***core FS purposes***. The draft Guidelines seem to conflate the exemptions in Article 22(2) with bases for processing under Article 6.[2]

Assuming that Article 22(2) refers to Article 6 in this way would result in the exemptions being unduly narrow, as is the case in the draft Guidelines.

The historic and ongoing interpretation of the Article 6 bases for processing is narrow and this is reflected in the draft Guidelines where page 12 references the 2014 WP29 opinion on legitimate interests. That opinion states for example:

- "The provision ['necessity for a contract'] must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some data processing is covered by a contract does not automatically mean that the processing is necessary for its performance." (Pages 16-17)
- "Fraud prevention - which may include, among others, monitoring and profiling customers - is another typical area, which is likely to be considered as going beyond what is necessary for the performance of a contract." (Page 17)
- "Credit reference checks prior to the grant of a loan are also not made at the request of the data subject under Article 7(b) [of Directive 95/46/EC and so cannot be based on 'necessity for contract'.]**"** (Page 18)

[2] Most explicitly on page 16.

If the current approach in the Guidelines of conflating Article 22(2) exemptions with Article 6 bases for processing is applied (together with narrow interpretation), this would strongly suggest that use of ADM for the ***core FS purposes*** could not rely on the exemption in Article 22(2)(a).

In fact though, Article 22(2) does not seem to refer to the Article 6 bases for processing, and certainly makes no explicit connection. Article 6 refers to the *processing* being necessary for the performance of a contract (etc). In contrast, Article 22(2) refers to the *decision* being necessary for this purpose.

The wording in Article 22(2) is more open than the wording in Article 6. To take an example: it may be true that the specific *processing* involved in taking a decision about whether to lend to an individual is not necessary for entry into the contract, as other processing could in principle be used (even if inefficient or less effective). Therefore, a different basis for processing under Article 6 may be more appropriate, e.g., legitimate interests. In contrast, the *decision* absolutely is necessary for entry into the contract, as it is impossible to make the loan without making a decision as to whether or not to do so.

Similarly, unlike Article 6(1)(b), Article 22(2)(a) does not refer to 'taking steps at the request of the data subject', suggesting that Article 22(2)(a) applies a different and more flexible test.

It is therefore valid and appropriate to distinguish between Article 6 and Article 22(2), which is worded more flexibly.

Recommendations:

- The Guidelines should be amended to make clear that the exemptions in Article 22(2) are not references to the bases for processing in Article 6.
- Page 12 should be updated to make clear that the 'performance of a contract' exemption can be interpreted more widely, including that Article 22(2)(a) refers to a *decision* (rather than specific processing) being necessary so as to enter into a contract.

'Authorised by Union or Member State law' needs to be explained

As noted above, firms use ADM in order to comply with rules and guidance from financial services regulatory authorities. As such, it is intuitively appropriate that the exemption in Article 22(2)(b) should apply.

However, this is not currently clear. The Guidelines do not explain how Article 22(2)(b) should be interpreted in any detail. They note that authorisations in law could cover monitoring to prevent fraud and tax-evasion, and maintenance of service security, but do not explain what an 'authorisation in law' means.

Where there is a statute which states that certain uses of ADM are permissible, or where an explicit legal obligation to use ADM for a certain purpose exists, this is relatively clear. However, in the context of financial services regulation in some jurisdictions this is seldom the case. Rather, regulatory authorities set high level obligations to (for example) 'maintain systems to detect and prevent financial crime', or to 'ensure responsible lending'.

In practice, firms comply with these obligations through the use of ADM, as this is the most effective and efficient means to meet regulators' expectations and ensure customers are protected.

However, it is unclear whether these kinds of *general* rules set by a regulatory authority could be considered 'authorisation in law' for ADM. As such, without further clarification in the Guidelines it is uncertain whether Article 22(2)(b) could be relied on to use ADM for the ***core FS purposes.***

This issue could be addressed perhaps through Member State legislation setting out authorisations for certain ADM. However, we are only six months from May 2018 and few Member States have finalised their legislative framework. As such, considerable uncertainty remains.

> **Recommendation**: The explanation of 'authorised in law' in the Guidelines should be expanded to make clear that the use of ADM for the purpose of supporting compliance with rules and guidelines from regulatory authorities is to be considered 'authorised in law'.

Explicit consent – not a viable alternative

The last exemption in Article 22(2) is where the Controller has the explicit consent of the data subject. This would seldom be possible in the context of the ***core FS purposes*** as, if this is the same test as for consent as a 'basis for processing', the consent would not be 'freely given' under Article 7.

A firm could not use consent as the basis for processing in this context, as this would allow the data subject to withdraw consent (and potentially also activate the Right to Erasure), putting the firm at risk of breaching its regulatory obligations and undermining the public interest objectives (fraud prevention, combating terrorist financing, maintenance of the financial robustness of the firm, responsible lending, etc).

As such, Article 22(2)(c) does not provide a practical alternative to the exemptions in (a) and (b) as set out above.

Summary of core recommendations: amendments should be made to the guidance on Article 22(2) to add flexibility and preserve the beneficial uses of ADM, as follows:

1) WP29 should consider carefully whether Article 22(1) should be interpreted as a prohibition.

If the prohibition interpretation is retained:

2) The Guidelines should be amended to make clear that the exemptions in Article 22(2) are not references to the bases for processing in Article 6.
3) Page 12 should be updated to make clear that the 'performance of a contract' exemption can be interpreted more widely, including that Article 22(2)(a) refers to a decision (rather than specific processing) being necessary so as to enter into a contract.
4) The explanation of 'authorised in law' should be expanded to make clear that the use of ADM for the purpose of supporting compliance with rules and guidelines from regulatory authorities is to be considered 'authorised in law'.

Additional issues

Pages 9 – 10 – human intervention

We query what is meant by 'oversight of the decision' by a natural person. Does this mean that a natural person must participate in *each decision*? In our view, comprehensive human oversight of, rather than an explicit need for participation in, the decision-making *process* would be more efficient, while still providing a high level of protection.

Pages 10 – 11 – 'legal' or 'similarly significant' effects

In our view, the phrase 'similarly significant effect' suggests that the effect or impact of a decision must be similar in nature and significance to a legal effect, which is a high threshold. In contrast, the draft Guidelines seem to interpret 'similarly significant effect' very widely, creating a very low threshold for ADM within scope of Article 22.

To highlight a few examples:

- At the bottom of page 10 the draft Guidelines suggest that a credit decision relating to renting a bicycle for two hours may be subject to Article 22.
    - In our view it is hard to see how a transaction of perhaps €5 would amount to a 'significant effect'. This suggests an extremely low threshold for Article 22.
    - More technically, it is not clear to us what the significant decision is here. Presumably this transaction would be via credit card (given the reference to credit in the Guidelines and Recital 71), in which case the decision would be the lender 'deciding' to process the transaction. This involves the customer drawing down on an existing credit facility under an existing contract and is very different from agreeing a *new* credit contract as is suggested in Recital 71. Use of an existing facility should be considered less significant than entry into a new contract.
    - **We suggest that either:**
        - **this example should be removed, or**
        - **this example should be amended to make clear that this not a sufficiently significant effect to come within Article 22.**
- On page 11 the draft Guidelines state that decisions to target certain advertising to an individual can be considered to have 'significant effects'.
    - We recognise that this could be the case in some extreme situations, such as targeting high cost credit to individuals who are overindebted, or attempting to identify problem gamblers so as to target them with gambling advertisements.
    - **We suggest that the Guidelines should make clear that more conventional / routine uses of targeted advertising are not caught by Article 22**.
    - We also note that in practice making an assessment as to the impact of advertising on a specific individual is likely to require extensive data gathering and analysis (contrary to the principle of data minimisation) if possible at all.
    - **We suggest that the Guidelines should make clear that the evaluation of the 'significance' of the effects should be based on the data available concerning the relevant target population as a whole.**
- On page 11 the Guidelines state that differential pricing could also have a significant effect on a customer.
    - Though this may be true in some scenarios, firms need somehow to determine the prices that they will charge a customer in order to be able to enter into a contract and manage their risk.
    - **We suggest that the Guidelines make clear that setting prices is within Article 22(2)(a).** (We highlight that the individual would be protected by the effective safeguards in Article 22(3) in this situation).
- An important use of profiling by firms is to understand customer behaviours and improve the design of products and services to better meet customer and commercial needs. **It would be useful for the Guidelines to clarify that this kind of profiling would be out of scope of Article 22, as there is not a decision in respect of an individual**.

As a broad point, we query whether Data Protection Authorities truly ought to (or wish to) regulate such diverse areas of the economy, beyond privacy issues. For example, law and regulation exists

already governing appropriate content and targeting of advertisements (for example Directive 2006/114 concerning misleading and comparative advertising). In financial services specifically, there are extensive requirements imposed at EU and Member State level to protect individuals, including to ensure that advertisements are appropriate and that lending decisions are fair.

We highlight that, although the Guidelines should be amended as suggested above to better clarify the threshold for Article 22, the issues we highlight in the first part of this submission would remain. If the threshold of Article 22(1) is raised, the exemptions will still need to be reconsidered to ensure that regulatory and other beneficial uses of ADM can continue.

Pages 8 and 9 – interaction between profiling and automated decision-making

The explanation on the bottom of page 8 concerning how the GDPR addresses profiling and ADM, and how these concepts interact, is not entirely clear. It should be revised to clarify that:

- Chapter III relates only to example (iii), being the only use of profiling subject to Article 22.
- Correspondingly, this explanation should be revised to make explicit that Chapter IV relates to all uses of profiling, including examples (i), (ii) and (iii), where applicable.

On page 9 the Guidelines state: "Chapter III of these guidelines explains the specific provisions that apply to solely *automated individual decision-making*, including profiling. A general prohibition on this type of processing exists to reflect the potentially adverse effect on individuals." [Our emphasis.]

Similarly, page 8, example (iii) refers to "solely *automated decision-making*, including profiling (Article 22)." [Our emphasis.]

This wording suggests that profiling is a type of 'automated decision-making' and that this is prohibited. However, this does not reflect the GDPR text. Article 22(1) refers to "…a decision based solely on *automated processing,* including profiling…" [our emphasis]. In other words, Article 22(1) (whether or not it is a prohibition) captures decisions based on *automated processing*, and gives profiling as an example the type of processing which *could* be automated and give rise to a decision.

> **We recommend amending pages 8 and 9 to better reflect the text in Article 22(1) of the GDPR.**

Pages 18 to 19 – Article 5(1) (b) Further processing and purpose limitation

The example on page 19 states:
"Some mobile applications provide location services allowing the user to find nearby restaurants offering discounts. However, the data collected is also used to build a profile on the data subject for marketing purposes - to identify their food preferences, or lifestyle in general. The data subject expects their data will be used to find restaurants, but not to receive adverts for pizza delivery just because the app has identified that they arrive home late. This further use of the location data may not be compatible with the purposes for which it was collected in the first place, and may thus require the consent of the individual concerned".

In this example **it should be clarified** that where building a marketing profiling was one of the initial purposes of collecting the data, this processing could also be based on legitimate interests, given Recital 47. Naturally, the controller would need to properly explain this additional purpose under Article 13.

The question of 'compatibility' is only relevant where the data are being *repurposed* after collection.

Pages 20 – 21 – Article 6(1) (b) – necessary for the performance of a contract

The example states:
"A user buys some items from an on-line retailer. In order to fulfil the contract, the retailer must process the user's credit card information for payment purposes and the user's address to deliver the goods. Completion of the contract is not dependent upon building a profile of the user's tastes and lifestyle choices based on his or her visits to the website. Even if profiling is specifically mentioned in the small print of the contract, this fact alone does not make it 'necessary' for the performance of the contract."

The Guidelines should make clear that this profiling could still potentially be based on legitimate interests.

ENDS