1 December 2017

**Comments by the Centre for Information Policy Leadership**

**on the Article 29 Data Protection Working Party's**

**"Guidelines on Automated Individual Decision-Making and Profiling"**

**adopted on 3 October 2017**

On 3 October 2017, the Article 29 Data Protection Working Party ("WP29") adopted its "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" (the "Guidelines"). The WP29 invited public comments on this document by 28 November 2017.[1] The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments below.

The GDPR specifically addresses profiling and automated decision-making (ADM[3]), two related but distinct activities, because they have the potential to impact individuals' rights and freedoms if carried out irresponsibly. CIPL recognises that the irresponsible application of profiling and ADM can directly result in unfair discrimination, financial loss, damage to reputation, social disadvantages and potential legal consequences for individuals. At the same time, profiling and ADM — provided they are carried out in a responsible manner — provide great benefits for individuals, society, organisations and the economy. Examples can be found in both the private and public sectors, for instance in healthcare, education, transport, banking, insurance and marketing.

Profiling and ADM have become essential to business and public sector operations in the modern digital information society. Their use will only increase with the fourth industrial revolution, the rise of artificial intelligence (AI) and machine learning and the overall increase in computing power. Indeed, automated decisions are being made more often and with increasing sophistication. If applied properly, the requirements of the GDPR, including those relating to profiling and ADM, will ensure appropriate protection for individuals while enabling society, individuals and organisations to reap the benefits of machine learning and other relevant technologies.

---

[1] An extension was granted for this submission until 5 December 2017.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 56 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

[3] In these comments, we use the terms "ADM" or "solely ADM" interchangeably to refer to solely automated decision-making covered by Article 22(1), i.e. solely automated decision-making that has a legal effect or similarly significant effect. Where automated decision-making not producing such effects is mentioned in this comment, this will be noted.

Given their increasing use, CIPL welcomes that the WP29 has made it clear that profiling and ADM are two distinct concepts, not regulated in the same way in the GDPR, and that the WP29 has developed practical guidance on each activity's application under the GDPR. In this paper, CIPL further considers profiling and ADM and offers suggestions for clarification with regard to certain aspects of these activities.

## A) The Proper Scope of Article 22

The role and function of Article 22 of the GDPR is to provide individuals with a heightened level of protection against solely automated decisions that produce legal or similarly significant effects on those individuals. Consistent with the risk-based approach, enshrined throughout the whole GDPR, the legislators' intent is to apply Article 22 to only the most impactful ADM where additional protection may be needed.

CIPL believes that the appropriate application of Article 22 can be achieved by:

- Interpreting the meaning of "legal" effect and "similarly significant" effect strictly, to ensure Article 22 only covers truly impactful ADM;
- Construing Article 22(1) as a right that may be invoked by the individual; and
- Recognising that Article 22 should not be considered in isolation as the only protection against solely ADM, but in combination with the other requirements and safeguards of the GDPR designed to protect individuals and ensure responsible use of data.

CIPL recommends that the WP29 reconsider one of the starting points of its analysis of Article 22(1), namely to present it as a direct prohibition, subject to three exceptions. CIPL believes that the direct prohibition interpretation:

- Is not mandated by the text of the GDPR;
- Is not necessary to provide the individual effective additional protection in situations where ADM could be risky;
- Would unnecessarily preclude certain types of beneficial, legitimate and safe automated decisions (see examples on page 10); and
- Greatly restricts the future-proof application of the GDPR to modern and evolving forms of data processing, including machine learning and AI, necessary for the development of new products and services in the EU Digital Single Market and the economic and societal progress of the EU.

CIPL believes that a right to be invoked interpretation of Article 22 is the correct interpretation as it is more consistent with the text of the GDPR and the legislative history

and is better suited to achieving the goals of the provision, namely to protect individuals while also facilitating modern data processing activities that provide benefits for individuals and society. This interpretation is also more consistent with the GDPR's overall emphasis on a risk-based approach.

## B) Comments[4] Regarding Automated Decision-Making

### 1. Interpreting Legal Effect and Similarly Significant Effect

#### 1.1. Meaning of Legal Effect and Similarly Significant Effect

***(See WP29 Guidelines — p. 10-11 "Legal" or "Similarly Significant" Effects)***

Article 22(1) applies to automated decisions[5] which produce legal effects or similarly significantly affect individuals. As a starting point, therefore, it is crucial that we have the correct understanding of what constitutes a "legal" effect and a "similarly significant" effect.

**Legal Effect**: This term is easier to apply and CIPL believes the WP29 has correctly described it as any "impact on someone's legal rights" or something that affects a person's "legal status or their rights under a contract". However, the example in the draft guidelines of an automated decision disconnecting someone from his or her mobile phone service for breach of contract because they forget to pay their bill before going on holiday should be reconsidered (see page 10 of the guidelines). Compared to the other examples in the guidelines (focused on societal benefits, denying border entry, or being subject to surveillance), the example appears trivial and in our opinion not strictly within the category of legal rights (individuals do not have a contractual right to a phone service if they do not respect their contractual obligations, such as, making timely service payments). Moreover, many companies have automated payment processing services constructed to determine simply whether customers have made payment, and do not consider extraneous factors when determining whether it is necessary and appropriate to cut off an individual's service. Such automation should not be considered problematic if the methodology is non-discriminatory and if individuals are able to understand why a decision has been made and to contest it.

**Similarly Significant Effect**: This term is more difficult to define. Initially, it is important to recognise that the term "similarly significant" is there for a reason. It means that **the effect**

[4] CIPL's comments do not strictly follow the order of the guidelines, but where our discussion addresses specific areas in the guidelines we provide the relevant headings and page number from the guidelines in bold and italics. Cross-references to pages of the guidance are further made within the text where relevant. Further, our comments are mostly limited to the issues the WP29 included in the guidelines and not a comprehensive discussion of profiling and ADM. As a result, we may not cover every important issue raised by these concepts and may seek to provide further input to the WP29 or other relevant body at a future time when and if useful and appropriate.

[5] The term "decision" itself has caused some debate. Some have argued that any action taken on a data set is a decision. For purposes of Article 22 of the GDPR, the only relevant decisions are those based solely on automated processing which produce legal effects or similarly significant effects on an individual.

**of a decision based on solely automated processing must be similar in its significance to a legal effect**. Thus, it is clear that the GDPR envisages **a high threshold** for decisions within the scope of Article 22. In fact, Article 22 is an example of the risk-based approach embedded in the GDPR — it recognises that some processing may be more risky and requires additional safeguards and rights. It also subjects such processing to a data protection impact assessment (DPIA) (Article 35(3)(b)).

The WP29 guidelines note that for a decision to produce similarly significant effects, the effects of the processing must be "more than trivial" and "sufficiently great or important" to be worthy of attention. CIPL welcomes the WP29's clarification that the effects of the processing must be sufficiently great or important to be worthy of attention. However, the "more than trivial" characterisation should be deleted or further clarified to reflect that any impacts must indeed be sufficiently great and have significant effects similar to that of a legal effect. "More than trivial" is a potentially very low threshold to meet and could encompass a whole range of solely automated decisions that do not rise to the level of being similarly significant to a legal effect or whose effects are "sufficiently great". Legal effects are clearly drastically more than trivial, and decisions producing similarly significant effects should have to meet the same threshold.

Additionally, CIPL recommends that the WP29's cross-reference to the concept of "substantially affects" as discussed in the WP29 guidelines for identifying a controller or processor's lead supervisory authority be removed. The reference is not relevant to the interpretation of Article 22. Firstly, one cannot transpose an interpretation in the context of jurisdictional issues to the completely different context of identifying which automated decision-making produces effects significantly impacting a data subject. Secondly, the list of types of processing that "substantially affects" individuals is overly broad for the purposes and rationale of Article 22, including processing that has "unlikely, unanticipated, or unwanted consequences" or "involves the processing of a wide range of personal data". The breadth of this list potentially increases the types of processing that would not otherwise fall under Article 22(1) and also diminishes the WP29's earlier statement that the effects of processing must be "sufficiently great or important to be worthy of attention".

Although the determination of what constitutes a "similarly significant" effect is highly contextual, CIPL believes that the following **non-dispositive criteria** could assist organisations to make the determination in cases where it is not clear if the automated decision produces such effects, keeping in mind the high threshold that needs to be reached:

- The temporary, prolonged or permanent impact of the automated decision on individuals;
- The severity and likelihood of risks and harms to individuals; and

- The impact of the automated decision at different stages of a decision-making process (i.e. does an initial or intermediary automated decision in a process produce a similarly significant effect or only the ultimate automated decision in that process).

**Recommendation: Clarify that for an ADM process to produce a similarly significant effect it must rise to the same level as producing a legal effect, which is a high bar. Delete the "more than trivial" characterisation and highlight that the similarly significant threshold is reserved for only the most impactful ADM. Delete the cross-reference to prior WP29 guidance in the context of the lead supervisory authority defining "substantially affects".**

### 1.2. Examples of "Legal" Effect and "Similarly Significant" Effect

Notwithstanding that the determination of "legal" effect or "similarly significant" effect is highly contextual, CIPL appreciates the WP29's list of examples of legal effects[6] (see page 10 of the guidelines).

However, organisations will need more clarity and consistency around the examples of automated decisions producing similarly significant effects. For instance, it is not clear whether all the examples of credit decisions (see pages 10 and 11 of the guidelines) reach the threshold of producing similarly significant effects. CIPL recommends that the WP29 clarify the examples and make clear whether each produces a similarly significant effect.[7] Similarly, CIPL does not believe that individual discounts based on loyalty create a similarly significant effect for individuals who are not recipients of the discount.[8] Finally, mere annoyance or inconvenience of individuals should not be a criterion for determining whether a decision produces a similarly significant effect. For example, it may annoy an individual that their phone or credit card is blocked on a certain occasion for fraud prevention purposes, but that inconvenience should not be factored into the determination of whether such blocking produces a similarly significant effect.

---

[6] Note however that CIPL disagrees with one example in this list. See discussion on page 3 of this comment regarding the WP29's example of an automated decision that means someone is automatically disconnected from their phone service for breach of contract because they forgot to pay their bill before going on holiday.

[7] For instance, one example put forward by the WP29 is an automated credit decision surrounding renting a city bike during a vacation abroad for two hours. While on the face of it a credit decision that prohibits someone from renting a bike for two hours does not seem to rise to the level of similarly significant effect, it would be impossible to make such a determination on an individual basis. For example, there could be factors specific to a single person that would lead one to conclude that not being able to rent a bike would have a significant effect. However, this would require an enormous amount of discovery and could in fact necessitate the need for the collection of additional personal data to make such a determination, which runs counter to the principles of data minimisation and proportionality. Therefore, impact determinations should generally be made on the basis of the average person or to the extent information is available to allow more bespoke determinations to be made.

[8] The guidelines note that ADM that results in differential pricing could have a significant effect if prohibitively high prices bar an individual from goods or services. However, this raises a host of questions including what defines prohibitively high prices given that each individual's financial situation is unique?

Providing good examples of automated decisions producing legal and significant effects can be useful to both large organisations and SMEs, particularly where the examples' parameters are clearly defined.

Based on wide input from organisations in different sectors, CIPL has prepared a table of examples of decisions which we believe could produce legal effects or similarly significant effects and of decisions we believe do not produce such effects. CIPL recommends that the WP29 create a similar table of examples.

| **CIPL Table on the Application Threshold of Article 22 GDPR** | |
|---|---|
| **Legal Effects** | • Decisions affecting the legal status of individuals;<br>• Decisions affecting accrued legal entitlements of a person;<br>• Decisions affecting legal rights of individuals;<br>• Decisions affecting public rights — e.g. liberty, citizenship, social security;<br>• Decisions affecting an individual's contractual rights;<br>• Decisions affecting a person's private rights of ownership. |
| **Similarly Significant Effects**<br><br>*Some of these examples may also fall within the category of legal effects depending on the applicable legal regime and the specific decision in question* | • Decisions affecting an individual's eligibility and access to essential services — e.g. health, education, banking, insurance;<br>• Decisions affecting a person's admission to a country, their residence or citizenship;<br>• Decisions affecting school and university admissions;<br>• Decisions based on educational or other test scoring – e.g. university admissions, employment aptitudes, immigration;<br>• Decision to categorise an individual in a certain tax bracket or apply tax deductions;<br>• Decision to promote or pay a bonus to an individual;<br>• Decisions affecting an individual's access to energy services and determination of tariffs; |
| **Decisions <u>Not</u> Producing Legal or Similarly Significant Effects**<br><br>*CIPL believes these automated decisions do not typically produce such effects. Instances where they might produce such effects are contextual and should be determined on a case-by-case basis.* | • Decisions ensuring network, information and asset security and preventing cyber-attacks;<br>• Decisions to sandbox compromised devices for observation, restrict their access to or block them from a network;<br>• Decisions to block access to malicious web addresses and domains and delivery of malicious emails and file attachments;<br>• Decisions for fraud detection and prevention (e.g. anti-fraud tools that reject fraudulent transactions on the basis of a high fraud score);<br>• Decisions of automated payment processing services to disconnect a service when customers fail to make timely payments;<br>• Decisions based on predictive HR analytics to identify potential job leavers and target them with incentives to stay;<br>• Decisions based on predictive analytics to anticipate the likelihood and nature of customer complaints and target appropriate proactive customer service;<br>• Normal and commonly accepted forms of targeted advertising;<br>• Web and device audience measurement to ensure compliance with advertising agency standards (e.g. requirements not to advertise foods high in fat, sugar and sodium when the audience consists of more than 25 % of children). |

**Recommendation: Where possible, clarify the existing examples of automated decisions producing legal and similarly significant effects and add the additional examples provided in the table above.**

### 1.3. Targeted Advertising — Not Similarly Significant to a Legal Effect

The comments in this section feature CIPL's key recommendations on the WP29's points about targeted advertising. For completeness CIPL has included a broader discussion of targeted advertising and its relationship with Article 22 as an annex to this paper.

CIPL welcomes and agrees with the WP29's acknowledgement that targeted advertising typically does not produce similarly significant effects on an individual. While the WP29 also suggests that "it is possible" that some targeted advertising may produce such effects, CIPL does not agree with the example presented in the guidelines to demonstrate this (i.e. someone in financial difficulties who is regularly shown online gambling ads and is induced into generating further debt) and recommends that the WP29 consider removing this example. The example raises the following difficulties:

- It is impossible for organisations to know the likelihood of whether their ad will have a significant impact on someone, especially without collecting and analysing additional information. Forcing organisations to make such determinations may compel the collection of more information.

- Most targeted advertising is conducted on an "interest-based" model whereby an individual is assigned to certain ad categories that correlate with his or her online activities. Such categories are often generic and do not reveal specific vulnerabilities of individuals (i.e. that someone may be in financial difficulties).

- If a controller obtained actual knowledge of an individual's vulnerabilities and attempted to target ads at the specific individual to exploit the vulnerability, such a practice (which would be extremely rare and outside the practice of normal advertising) would be caught by the risk-based approach of the GDPR. It would require an advertiser to weigh the risks and harms of such a processing operation against the benefits. In such cases, the advertiser would be required to stop the processing and not proceed with the targeted advertising.[9]

CIPL recommends that the WP29 amend the four factors it presents as criteria to consider in determining whether an ad produces similarly significant effects, in order to create a more

[9] Also, it is questionable whether specifically targeting people to exploit their vulnerabilities would not involve the decisional participation of a human. For a controller to have actual knowledge of these vulnerabilities it would have to take measures to obtain this data, as ad interest categories alone are unlikely to reveal this (e.g. buying lists of individuals in financial difficulties through data brokers). Such affirmative action involves the controller in the decision-making process to specifically target these individuals with certain ads and arguably brings this type of activity out of the realm of solely automated processing for the purposes of Article 22 of the GDPR.

pragmatic approach. The factors as they stand will create further confusion and a lack of legal certainty among controllers. They may completely diminish the benefits of targeted advertising for individuals and lead to substantially negative impacts for advertisers for the following reasons:

- **The intrusiveness of the profiling process**: Intrusiveness is a broad and subjective notion. Profiling practices that are outside the remit of normal and commonly accepted advertising practices may be considered as too intrusive depending on context. Nevertheless, such practices would undergo a risk assessment to balance the benefits and harms of such processing.

- **The expectations and wishes of individuals concerned**: CIPL questions how this criterion would be implemented in practice. The expectations and wishes of individuals are highly subjective and impossible to predict in the absence of some affirmative action on the part of the individual. Moreover, many online services provide ad management tools for individuals to remove themselves from ad categories, to add new categories to their profile or to turn off targeted ads completely. These tools empower individuals to manage their own wishes and expectations for targeted ads.

- **The way the advert is delivered**: This criterion is overly broad as ad delivery can take numerous forms (e.g. pop-ups or ad displays on the side of a browser window). On one end of the spectrum, ads delivered through deceptive means, are illegal and/or would not survive a risk assessment, as required by the GDPR. However, normal and commonly accepted ad delivery methods do not rise to a level of producing a similarly significant effect.

- **The particular vulnerabilities of the data subjects targeted**: As outlined above, it is impossible for advertisers to know in advance whether an individual is particularly vulnerable to certain ads without collecting a great deal of additional information about the individual.

**Recommendation: Remove the example put forward to demonstrate a targeted ad producing a similarly significant effect (i.e. someone in financial difficulties who is regularly shown online gambling ads and is induced into generating further debt). Amend the four factors to consider in determining whether an ad produces a similarly significant effect, in order to create a more pragmatic approach.**

## 2. Article 22 — Direct Prohibition or Right to Invoke?

***(See WP29 Guidelines — p. 9 Specific Provisions on Automated Decision-Making as Defined in Article 22)***

### 2.1. Direct Prohibition

One of the most significant issues raised by the WP29 guidelines is the correct interpretation of Article 22(1) of the GDPR — i.e. whether Article 22(1) should be viewed as a direct prohibition or a right to be invoked by individuals. The WP29 interprets Article 22(1), the "right not to be subject" to ADM, as a general prohibition against conducting ADM unless an exception under Article 22(2) applies.

However, the direct prohibition interpretation is, in our opinion, not correct and is not mandated by the text or legislative history of the GDPR (see discussion on pages 14 and 15). Furthermore, the direct prohibition interpretation is too restrictive to ensure that the GDPR remains principle-based and future-proof in light of evolving data processing, machine learning and AI. Such an approach would result in unnecessarily subjecting an increasing amount of machine learning-based processing to individual consent or necessity for performance of a contract.

Moreover, the approach eliminates legitimate interest, public interest and vital interest as valid bases for carrying out ADM, including a broad range of established and accepted processing practices (see discussion on page 10). Processing necessary for the performance of a contract, compliance with a legal obligation or consent are not "better" grounds for processing than any of the other grounds, nor are they necessarily more protective of individuals' rights.

As we explained in CIPL's paper on Transparency, Consent and Legitimate Interest,[10] the GDPR essentially places all processing grounds on equal footing while recognising, of course, that different grounds may be appropriate for different contexts. Thus, it can be argued that in many contexts, a strong legitimate interest assessment coupled with a robust approach to allowing individuals to invoke their right not to be subject to automated decisions producing legal effects or similarly significant effects may deliver equal, if not stronger, protections to individuals. This is because the legitimate interest ground requires a well-documented, context-specific risk/benefit assessment. This includes a balancing of competing interests and rights, strong technical and organisational controls around the use of algorithms and the implementation of mitigations as part of organisational accountability.

Under the direct prohibition interpretation, to engage in ADM, organisations will have to obtain a specific and explicit consent from individuals or alternatively demonstrate that such

[10] http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

processing is necessary for the performance of a contract. This raises several difficulties in the implementation of Article 22 of the GDPR:

a) Over-reliance on consent is unnecessarily restrictive — it can lead to consent fatigue, erode effective protection for individuals and prevent many types of legitimate and safe data processing that increasingly involve ADM;

b) There may be instances where it would be prejudicial to seek consent and enable any choice for individuals. For example, in cases of ADM performed by banks, credit card and payment processors or their data processors for the detection and prevention of anti-money laundering or anti-terrorism financing;

c) Necessity of contract as a processing ground, both in the GDPR generally and for ADM specifically, is also restrictive and is often interpreted very narrowly by DPAs. Even though there may be good reason to carry out ADM, unless such decision-making is necessary to perform or complete a contract, it is prohibited; and

d) The direct prohibition interpretation severely limits the ability to engage in certain forms of legitimate ADM, where consent may not be viable or contractual necessity not applicable, but legitimate interest would be a viable ground. For instance:

- Anti-money laundering and know your customer screening, including understanding "vulnerable" customers (where not pursuant to national or EU law but based on requirements by financial regulators, telecommunications, energy or other regulated industry oversight bodies);
- E-recruitment decisions where ADM processes select people to advance in a recruiting process based on objective criteria and pre-determined factors;
- ADM based on online testing and pre-screening of candidates for university admissions, internship and job applications, language proficiency etc;
- Use of ADM for educational uses, especially in distance learning, to help teachers deliver specific personalised modules, based on what pupils know and what they need; and
- Health and safety screening of employees at industrial plants.

Given the obvious limitations of restricting Article 22 to only three processing grounds, CIPL believes that ADM should be possible under legitimate interest, vital interest or public interest[11] processing grounds. This is strengthened by the fact that the GDPR provides many

[11] As an aside, the WP29 should clarify on page 21 of the guidelines under point 4 (Article (6)(1)(d) — necessary to protect vital interests) that if processing data for important public interest grounds, the controller must meet the requirements of Article 9, and in particular Article 9(2)(c) or 9(2)(g). Only 9(2)(c) is currently referenced.

safeguards to protect individuals against the consequences of such decisions in addition to their Article 22 right not to be subject to ADM.

Thus, CIPL appreciates the WP29's recognition that the GDPR offers many other protections and organisational accountability requirements[12] applicable to ADM. CIPL recommends the WP29 further emphasise and acknowledge that Article 22 should not be looked at in isolation, but together with the entirety of these other GDPR safeguards and requirements that further ensure individuals are protected from the risks of solely automated decisions.

Given the far-reaching consequences of the direct prohibition interpretation on a multitude of legitimate and beneficial forms of ADM, it is crucial that the remaining conditions of Article 22(1) be interpreted narrowly. The threshold of applicability of Article 22 must remain high — only those instances of **solely ADM that produce legal or similarly significant effects** on individuals must be affected by the prohibition.

However, a more effective measure and perhaps more in line with the spirit of individual rights than the "direct prohibition" interpretation would be the alternative "right to be invoked" interpretation of Article 22(1), which is discussed below.

**Recommendation: Reconsider the direct prohibition interpretation and interpret Article 22(1) as a right to be invoked (see discussion below). Highlight the importance of organisational accountability and other GDPR protections in relation to ADM.**

### 2.2. Right to be Invoked and the Essence of the Right Not to be Subject to ADM

To facilitate the implementation of Article 22, CIPL believes Article 22(1) should be interpreted as a right to be invoked by individuals where ADM produces legal or similarly significant effects. When the right is invoked, the protection of Article 22 would apply, in addition to all other relevant GDPR safeguards.

Under this interpretation:

a) solely ADM would be permitted

b) unless the individual invokes a right not to be subject to ADM prospectively before the decision, except where the exceptions in Article 22(2)(a), (b) or (c) apply (no prospective objection possible)

[12] These include: (i) compliance with the data protection principles outlined in Article 5 of the GDPR; (ii) ensuring there is an appropriate legal basis to engage in ADM under Article 6 and compliance with the rules on processing of special categories of data under Article 9, as well as, Article 22(4) of the GDPR; (iii) ensuring compliance with the transparency and notice requirements of Articles 12 through 14; (iv) the risk-based approach, that requires organisations to understand and assess risks and harms to individuals throughout the compliance lifecycle and conduct a data protection impact assessment (DPIA) under Article 35 for areas of high risk; and (v) rules on cross-border transfers under Chapter V of the GDPR. In addition, individuals retain all their rights under the GDPR (outside of their Article 22 right not to be subject to ADM), for example, their right of access, correction and erasure and the right to object to profiling in Article 21. Article 12(2) further states that the controller must facilitate individuals in the exercise of their rights (see discussion below on page 14).

c) the individual can also invoke the right retrospectively after the decision is made in any ADM context regardless of processing ground, including where the exceptions in 22(2)(a) or (c) apply[13]

d) if invoked, an individual can no longer be subject to solely automated decisions producing legal or similarly significant effects unless an exception under Article 22(2) applies

e) if an exception applies, then the additional safeguards provided by Article 22(3) apply.[14]

To illustrate this process, CIPL has prepared an ADM right to be invoked interpretation flowchart. We recommend including a similar visual flowchart to assist organisations in identifying the requirements of ADM under the GDPR in the revised WP29 guidelines.

[13] Where the processing grounds are not consent or necessity of contract but, for example, legitimate interest, the individual can also assert his or her right not to be subject to ADM retrospectively. In such cases, the organization would be required to facilitate this right under Article 12(2), presumably, for example, by providing some form of human review.

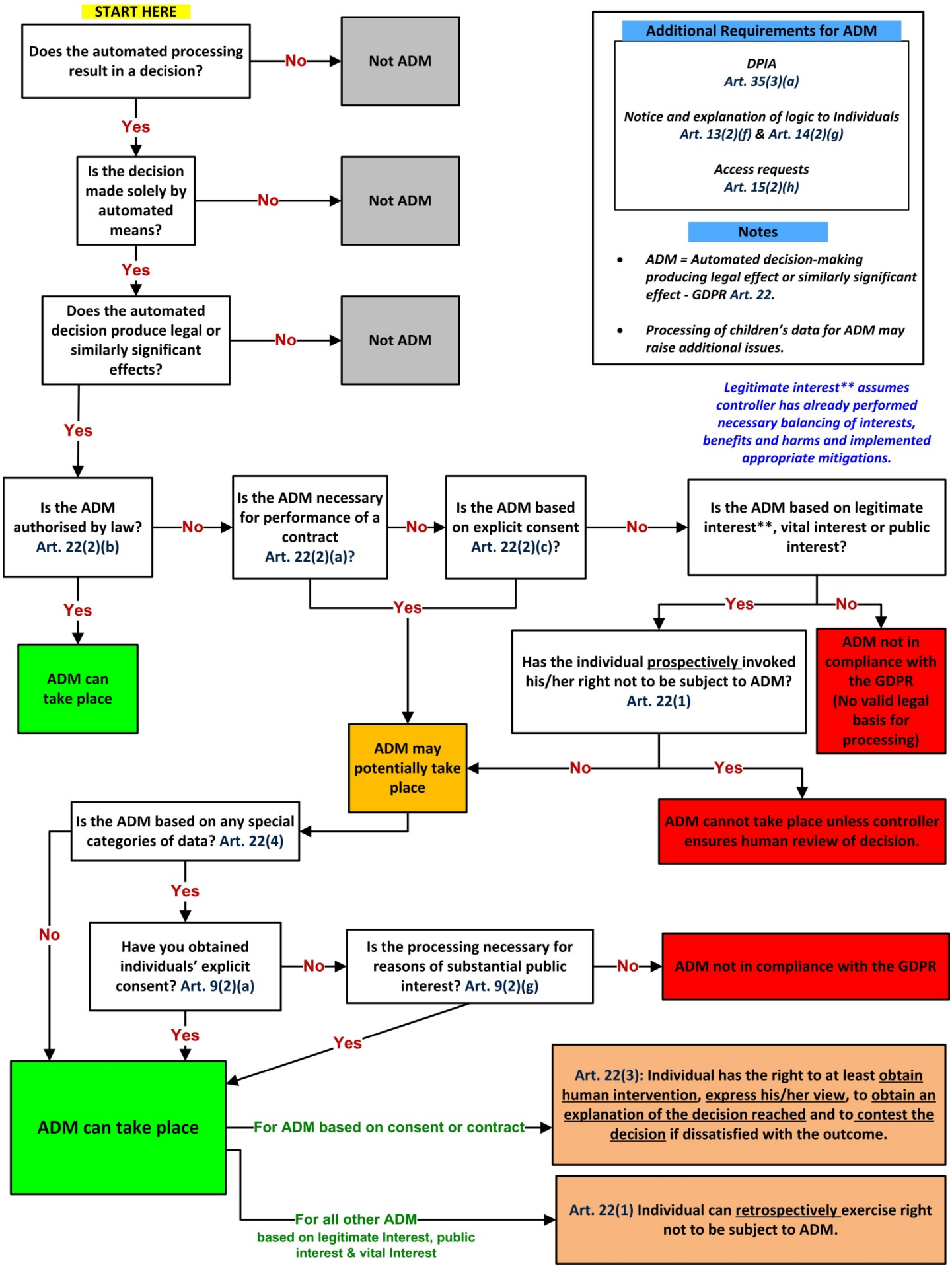
[14] The GDPR provides that no review is available if the decision is authorised by law. However, such laws must include "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." Article 22(2)(b).

Centre for Information Policy Leadership
Hunton & Williams LLP

1 December 2017

# Automated Decision-Making (ADM) Flowchart

## Article 22 as a Right to be Invoked



CIPL believes that this interpretation would be in line with the **spirit and the essence of the right** in Article 22, which in our view consists of the right of the individual to:

a) demand human intervention;

b) express his or her point of view;

c) receive an explanation of how the decision was made;

d) demand corrections; and

e) contest a decision.

This right in Article 22, in its essence, is different from the right to object to processing, including profiling, in Article 21 (which exists as a separate individual right in any case).

There exists much support for the interpretation that Article 22(1) is a right to be invoked:

- **Other data subject rights in the GDPR require affirmative action**: Individuals must invoke other GDPR rights. Other rights under the GDPR state that the data subject "shall have the right … to [something] …."[15] If Article 22(1) is also a right, then it too must be invoked. It is a right for the individual to do something in order not to be subjected to ADM producing legal or similarly significant effects.

- **The controller must facilitate individuals' rights under Article 12(2)**: Article 12(2) of the GDPR states that "the controller shall facilitate the exercise of data subject rights under Article 15 to 22". This only makes sense if Article 22 is a right to invoke. If controllers are not allowed to engage in ADM under Article 22(1) then they can never facilitate individuals in exercising their right not to be subject to automated decisions producing legal or similarly significant effects under Article 22(1).[16]

- **Article 22 is included in Chapter III**: The legislator included this right in Chapter III of the GDPR on individual rights. Under the direct prohibition interpretation, the controller is under an obligation not to engage in ADM unless an exception applies. This raises the question of why such an obligation would not be included under Chapter II of the GDPR which outlines the principles relating to the processing of data or Chapter IV on controller and processor obligations if Article 22 was intended to be a prohibition.

[15] For example: (i) Articles 15-18 which state "The data subject shall have the right to obtain…"; (ii) Article 20 which states "The data subject shall have the right to receive…"; and Article 21 which states "The data subject shall have the right to object…."

[16] Indeed, if an exception exists under Article 22(2), then the right under Article 22(1) does not apply at all ("Paragraph 1 shall not apply"). Thus, under the "direct prohibition" approach, there will never be an instance where the data subject can exercise their right under Article 22(1) pursuant to Article 12(2) even though Article 12(2) says the controller must enable them to do so. This strongly suggests that the GDPR envisions the "right to be invoked" interpretation.

- **GDPR drafting history**: Had the legislator intended the right to be a prohibition on the controller, they would have explicitly stated this and made it subject to exceptions. For example, Article 9 (1) explicitly states that processing of special categories of data shall be prohibited and the exceptions to this rule follow. The same is the case in relation to the prohibition on international data transfers under Article 44. Moreover, the original Commission proposal and the report from the LIBE Committee during the legislative process included language that clearly sways more in favour of a direct prohibition approach. The original text read "Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in Article 20(1) only if the processing…is based on performance of a contract, authorised under law, or explicit consent". Why was this language changed in the final GDPR text if a direct prohibition approach was intended?

- **Implementation of Article 15 of the Directive**: Article 15 of the Directive, which deals with automated individual decisions, was viewed in a different way across the EU, with some member states implementing it as a right to be invoked. The Directive was passed at a time when ADM and machine learning was an exception and not a normal data practice. Today these activities are more prevalent and we must consider that the GDPR has to be suitable for the next digital era where decisions will be made by machines. Hence, ADM cannot be prohibited outright.

- **Other GDPR protections apply to ADM**: Under a right to be invoked interpretation, all other GDPR protections continue to apply in respect of automated decisions producing legal or similarly significant effects.[17] The rules on transparency and notice disclosures are of particular importance, and further ensure protection of the individuals as they relate to ADM. Under the notice requirements of Article 13 and 14 and the access provisions of Article 15, controllers must inform individuals of the existence of ADM and, at least in those cases, provide meaningful information about the logic involved and the significance and the envisaged consequences of such processing for the individual. This requires that controllers notify individuals that ADM is taking place and provide information about how it may impact them. Furthermore, Article 12(2) of the GDPR requires that the controller facilitate the exercise of data subject rights under Article 15 to 22. Controllers engaged in ADM will have to ensure that individuals are notified of how they can invoke their right not to be subject to ADM and through what mechanism.

- **Suitability to modern and evolving data processing**: The right to be invoked interpretation is more in line with modern and evolving data processing activities. If organisations were unable to engage in ADM effects without individuals' explicit consent, authorisation by law or necessity for the performance of a contract, they would be forced to revisit and potentially cease certain completely legitimate and safe data processing and machine learning applications. For example, organisations

[17] See Footnote 12.

may receive thousands of job applications, and it is not possible for an organisation to manually review each and every application both in terms of the feasibility of the review (time and effort) and performing a totally unbiased review (i.e. maintaining 100 % objectivity and reviewing each application on an even playing field). See discussion on page 10 for additional examples.

**Recommendation**: **Adopt the "right to be invoked" approach to Article 22, acknowledging that it is equally protective of individuals, more realistic, workable and practical for both individuals and organisations and more accurately aligned with the other provisions of the GDPR.**

## 3. Additional Issues Related to ADM

### 3.1. Using Data to Train Machine Learning Models and Algorithms

***(See WP29 Guidelines — p. 12 Exceptions from the Prohibition)***

The WP29 guidelines note, under the direct prohibition viewpoint, that ADM can only take place under the Article 22(2) exceptions.

CIPL recommends that the WP29 clarify the position on using training data to build, improve and enhance algorithms. Organisations that are creating new algorithms often use personal data to input information into their ADM processes to test and refine them to ensure they are accurate, fair and dependable. Where possible, to minimise the potential privacy impact on any individual data subject, many organisations de-identify testing data by using robust procedures such as data scrubbing, or they may try to use pseudonymised data. In addition, administrative and contractual controls can be employed to further minimise risk.

It is important to ensure that training of machine learning models can take place, especially as these processes and tools are precisely meant to ensure fairness and the proper functioning of algorithms and ultimately protect individuals. The WP29 should clarify that such practices are exempt from Article 22 of the GDPR and can take place on the basis of legitimate interest, because there is not a decision that is actually carried through in respect of any individual.

**Recommendation**: **Clarify that using data to train or enhance algorithms is exempt from the requirements of Article 22 of the GDPR, once the organisation has made efforts to sufficiently de-identify the training data where possible and employ other risk minimising controls where appropriate and necessary (e.g. administrative and contractual controls)**.

### 3.2. Meaningful Information About the Logic Involved

***(See WP29 Guidelines — p. 14 Meaningful information about the "logic involved")***

Articles 13(2)(f) and 14(2)(g) of the GDPR state that when ADM takes place, individuals should be provided with meaningful information about the logic involved, as well as the

significance and the envisaged consequences of such processing for the data subject. CIPL welcomes the WP29's clarification that the controller should find simple ways to inform the data subject about the rationale behind, or the criteria relied on in reaching the decision without necessarily providing a complex explanation of the algorithms used or disclosure of the full algorithm.

Full transparency of algorithms (i.e. disclosure of source code or extensive descriptions of the inner workings of algorithms, including scoring models) is not meaningful to users and does not advance their understanding of how their data is being handled in ADM processes. Extensive explanations of algorithms may in fact confuse and overwhelm users due to information overload.

In addition, full transparency of algorithms raises intellectual property and trade secret issues for organisations, just like the disclosure of other types of proprietary information, such as software and patents. Protecting algorithms from full disclosure is vital for technological innovation. Finally, maintaining a minimum level of opaqueness surrounding how algorithms operate is necessary to prevent individuals from manipulating the algorithm unethically or illegally for personal gain (e.g. an individual who is able to obtain full disclosure of the algorithmic process and criteria for deciding who to audit for tax purposes). This is comparable to situations where the security of processing would be put at risk if full transparency of security measures and protections are made to bad actors.

**Recommendation: Clarify that extensive or full disclosure of the workings of an algorithm is unlikely to provide an individual with meaningful information. Recognise that algorithmic transparency must be limited in order to respect intellectual property rights and to prevent the unethical or illegal manipulation of algorithms.**

### 3.3. What is Human Intervention?

***(See WP29 Guidelines — p. 15 Right not to be subject to a decision based solely on automated decision-making)***

The WP29 guidelines state that to qualify as human intervention 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.

CIPL welcomes the WP29's explanation and elaboration on the meaning of human intervention. Human intervention can take more than one form and depends on the specific nature and context of the ADM. It can occur any time in the process, not just at the point of review of a decision.

Human intervention may involve a review of the ADM process (i.e. the workings of the algorithm), or the review of the input and output of the automated processing. Moreover, the WP29 should clarify that the ultimate goal of human intervention should be to assess

the correctness of the automated process and the fairness and accuracy of a particular decision under the circumstances. This goal determines which specific human intervention steps must be taken in a given situation. All of the above should result in a decision not being taken solely by automated means and would take the decision outside the scope of Article 22.

Finally, human intervention must be related to a specific instance of ADM for which the individual is invoking his or her right.

**Recommendation: Clarify that the nature and scope of human intervention is highly contextual and can include a range of measures. The ultimate goal of human intervention should be to ensure correct automated processing and a fair and accurate decision. Human intervention must relate to a specific instance of ADM.**

### 3.4. Best Practices and Safeguards

***(See WP29 Guidelines — p. 28-30 Good practice recommendations for profiling and automated decision-making)***

The WP29 outlines valuable good practice recommendations for controllers to address the GDPR requirements on profiling and automated decision-making. Indeed, CIPL believes that good practices should be the biggest focus of the guidelines, in line with the overarching accountability principle in the GDPR. Thus, CIPL encourages the WP29 to add more examples of best practices from the feedback it receives. In particular, CIPL recommends the WP29 clarify some of the existing best practices and add the following additional best practices to the guidelines:

- **Right of Access**: The guidelines note that where a data subject exercises his or her right of access in relation to profiling or ADM processes, information about the categories of data that have been or will be used in the process should be provided. This information will be more relevant than providing complex mathematical explanations about algorithms and machine learning. The guidelines further note that controllers should provide in addition to details about a profile, the sources used to develop it. CIPL believes the WP29 should further clarify that the results of an analytical process are not included in the scope of the right of access. This is consistent with the ruling of the European Court of Justice in *YS v Minister voor Immigratie*.[18]

  Furthermore, the WP29 guidelines refer to Recital 63 which mentions that the right of access "should not adversely affect the rights or freedoms of others", which is relevant for controllers concerned about revealing trade secrets or intellectual property (see page 24 of the guidelines). The WP29 states that only in rare circumstances should these rights outweigh individuals' rights of access. While CIPL agrees that controllers should not use Recital 63 as an excuse to deny access or refuse to provide information to

[18] Case C-141/12 *YS v. Minister voor Immigratie, Integratie en Asiel*, ECLI:EU:C:2014:2081.

individuals, we recommend the WP29 revise the statement to emphasise that the determination of whether a controller's rights and freedoms would be adversely affected by honouring an access request is contextual. An appropriate balance must be struck, taking into account all relevant factors. Trade secrets and intellectual property are relevant factors and are essential for many companies in the digital economy. Therefore, we recommend the WP29 remove the reference to "rare circumstances".

- **The Role of the DPO:** The DPO has an important role to play in ensuring accountability of the ADM process. This includes working collaboratively with data scientists and engineers, raising awareness and providing training about the risks of specific profiling or ADM, developing and evangelising best practices on algorithmic accountability, engaging in the design of the process and leading risk and benefit assessment processes.

- **Risk Assessment:** Before deploying a new profiling or ADM process, organisations must identify potential risks and harms associated with the process and take appropriate steps to mitigate such harms. For example, if a risk assessment shows that an ADM tool yields biased results, the organisation, having conducted a risk assessment to determine this, can recalibrate the specific ADM model to ensure fair outcomes. Use of datasets to train the algorithm and test the recalibration should be permitted (see discussion above on page 16). This preliminary step is key before deploying new profiling and ADM processes. As the WP29 outlines in its guidelines, conducting regular quality assurance checks and algorithmic auditing after a profiling or ADM process has been deployed also constitutes two important best practices.

**Recommendation**: **Clarify existing and add further examples of organisational best practices.**

## C) Comments Regarding Profiling

### 1. What Constitutes Profiling

#### 1.1. Stages of Profiling

***(See WP29 Guidelines — p. 6-7 Profiling)***

The guidelines refer to the definition of profiling under the Council of Europe Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling[19] (the "Recommendation"), noting three distinct stages of profiling: i) data collection; ii) automated analysis to identify correlations; and iii) applying the correlation to an individual to identify characteristics of present or future

[19] Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum. Council of Europe 23 November 2010. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf.

behaviour. According to the guidelines, "[e]ach of [these] stages represents a process that falls under the GDPR definition of profiling" (emphasis added).

The WP29 should clarify that while each stage of profiling under the Recommendation represents a process falling under the GDPR definition of profiling, processing must have taken place in all three stages, before the processing equates to profiling under the GDPR. The essence of profiling is more than the collection of personal data for the purpose of later evaluation. It also requires that the information is actually used to make evaluations, in particular analyses or predictions, about personal aspects of individuals. Looking at the wording of Article 4(4) of the GDPR, profiling is limited to "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects…." (emphasis added). The term "use of data" suggests that the evaluation must be presently occurring for there to be profiling.

In addition, the guidelines note that profiling has to involve some form of automated processing, but human involvement does not necessarily take the activity out of the definition (see page 6 of the guidelines). CIPL disagrees with this premise. The GDPR states that profiling consists of "any form of automated processing". This does not include manual processing. In other words, if the collection and evaluation, analysis and prediction are conducted manually, then the activity does not amount to profiling.

Nevertheless, should the WP29 maintain the position that some manual processing does not take the activity out of the definition of profiling, CIPL recommends it clarifies that in order to fall under the definition of profiling, it is the actual use of the data to evaluate, analyse or predict personal aspects that has to be automated. Where data is collected by automated means, for example in online forms, and the subsequent evaluation, analysis or predictions are conducted manually, this should not equate to profiling, as the core activity (i.e. the evaluation) is not automated processing. This would not amount to ADM either, as the activity is not solely automated.

**Recommendation: Make clear that processing only falls within the definition of profiling under the GDPR if collected personal data is actually used to evaluate, analyse or predict personal aspects relating to a natural person. Clarify that manual evaluation, analysis or prediction of personal aspects relating to a natural person does not equate to profiling. Such activities must be conducted by fully automated means to fall within the definition.**

### 1.2. Types of Profiling

The WP29 guidelines note that there are three types of profiling (see page 8 of the guidelines) — (i) general profiling; (ii) decision-making based on profiling; and (iii) solely automated decision-making, including profiling (Article 22). The guidelines then note that although there are three types, only two legal frameworks apply. This statement and the wording used are confusing. The GDPR does not contain specific requirements for decision-

making based on profiling that is not solely automated. Also, the wording in point (iii) above should not be "solely automated decision-making, including profiling", but profiling that results in a solely automated decision which produces legal effects or similarly significantly affects an individual. The WP29 should revise this section and make clear that there are two types of profiling: (i) general profiling, which can include non-solely automated decision-making, subject to all the requirements of the GDPR and (ii) profiling that results in a solely automated decision which produces legal effects or similarly significantly affects an individual, which is also subject to all the requirements of the GDPR and the additional provisions of Article 22.

**Recommendation: Make clear that there are two rather than three types of profiling — (i) general profiling and (ii) profiling that results in a solely automated decision which produces legal effects or similarly significantly affects an individual.**

### 1.3. Examples of Profiling in Current Use and Its Benefits in Different Industries

Profiling has become a fundamental part of business and public sector practices and is often used as a decision-making tool to support all kinds of internal and external decisions. CIPL suggests that the WP29 provides an illustrative list of examples of profiling usage in the digital economy. This will demonstrate its societal presence and aid organisations in determining whether their own activities fall within the definition of profiling. CIPL has prepared a table of such profiling examples in different industries which may provide a helpful starting point:

| **CIPL Table of Profiling Uses in Different Sectors** | |
|---|---|
| **Sector** | **Profiling is used for:** |
| Banking and Finance | • Credit scoring and approval;<br>• Ensuring responsible lending;<br>• Customer segmentation to ensure appropriate product offerings and protections;<br>• Initiatives to know your customer;<br>• Preventing, detecting and monitoring of financial crimes;<br>• Debt management;<br>• Credit and risk assessments;<br>• Fraud prevention;<br>• Anti-money laundering efforts;<br>• Preventing the financing of terrorism;<br>• Detecting tax evasion;<br>• Countering bribery and corruption;<br>• Preventing cybercrimes. |
| Health | • Greater efficiency and precision in delivery of healthcare and medicines<br>• Increasing the accuracy of diagnoses;<br>• Understanding syndromes and preventing recurrence;<br>• Understanding links between particular symptoms and medicines;<br>• Ensuring quality performance of physicians and medical staff. |

| | |
|---|---|
| Information and Network Security | • Cyber-incident prevention and diagnostics;<br>• Network and information protection;<br>• Personalisation of Internet browsing sessions. |
| Insurance | • Underwriting risks and allocating premiums. |
| Human Resources | • Recruitment and the objective analysis of job applications;<br>• Examining employee retention patterns;<br>• People development and promotion;<br>• Unlocking unused employee skills and abilities;<br>• Obtaining insights into employee performance drivers;<br>• Monitoring compliance with internal policies, codes of conduct and business ethics;<br>• Screening for compliance with export control and economic sanctions laws;<br>• Promotion of workplace diversity and inclusion. |
| Energy | • Predicting energy consumption;<br>• Forecasting demand and supply levels;<br>• Understanding usage peaks;<br>• More efficiently detecting and responding to utility outages. |
| Education | • School and university admissions;<br>• Promoting policies of affirmative action;<br>• Using analytics to optimize learning environments. |
| Marketing | • Providing recommendations based on profiles, previous and peer purchases;<br>• Loyalty programs – retail, hotel, travel services, etc.;<br>• Customer segmentation. |
| Non-Profit | • Identifying potential supporters and patterns of charitable behaviours. |
| Public Sector | • Detection of tax evaders;<br>• Detection of social security and benefits fraud;<br>• Focusing resources on appropriate cases for investigation;<br>• Policing and law enforcement;<br>• Public health and safety – predicting trends and preventing accidents. |

**Recommendation: <u>Provide more examples of profiling in the digital context, highlighting its increased commonality in the marketplace and use in a variety of different industries and the public sector</u>.**

### 1.4. Effects of Profiling

***(See WP29 Guidelines — p. 5 Introduction)***

The WP29 guidelines note that profiling can "lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds". This statement does not take into account that many individuals are given control over their profiles and can add, edit and delete from them. For example, if an individual is profiled as someone interested in sports and receives ads for books about sports, they are not necessarily prevented from seeing ads for any other types of books. They are simply more

likely to see ads for sports books. In addition, if the individual would like to see ads for non-sports-related books they can simply remove this ad category from their profile or indicate that they are interested in seeing ads about books in general and from all genres.

Furthermore, profiling an individual results in that individual seeing recommendations for certain goods or services. The individual is free to decline recommendations and look for other goods or services separately. In a non-advertising context, if a consumer is profiled as a high credit risk and is offered certain financial products based on this, the individual can check their credit report to see if the information in their profile is correct and if not, amend it. If the high credit risk rating is correct, the individual can always search for financial products and services aimed at low to moderate risk customers. Their freedom to choose other services is not restricted.

**Recommendation**: **The WP29 guidelines should make clear that profiling does not undermine an individual's freedom to choose certain products or services, with the exception of extreme circumstances. Most forms of profiling and targeted advertising based on profiles do not restrict an individual's freedom to choose certain products or services.**

### 1.5. Storage Limitation

***(See WP29 Guidelines —p. 19-20 — Article 5(1)(e) Storage Limitation)***

The WP29 guidelines state that "storing collected personal data for lengthy periods of time means that organisations will be able to build up very comprehensive, intimate profiles of individuals, since there will be more data for the algorithm to learn…storing [the data] for a long time may conflict with the proportionality consideration…[and] keeping personal data for too long also increases the risk of inaccuracies".

Firstly, CIPL believes that the WP29 should emphasise that while data should not be kept for longer than necessary under Article 5(1)(e) of the GDPR, personal data can be retained for as long as "necessary for the purposes for which the personal data are processed". This should not be different for profiling or automated decision-making. Secondly, the WP29 should acknowledge that in the case of profiling, storing data for longer periods will be advantageous to data subjects as the technology behind profiling is such that the more data is taken into account by the profiling algorithm, the more accurate the profiling will be. Finally, the words "lengthy periods" and "too long" in the guidelines above are vague. It is unclear who will determine what duration of time is too long or lengthy. This can result in scenarios where even if the data is still necessary for the processing, a data controller could be deemed as holding it for too long and be required to delete it. Such a determination has two consequences: (i) the profiling would become less accurate and (ii) data subjects would suddenly be confronted with their data no longer being recoverable.

**Recommendation: Emphasise that Article 5(1)(e) applies to profiling and automated decision-making just like it does to all other forms of processing. Personal data can be**

**retained for as long as necessary for the purpose of processing. Acknowledge the advantage of retaining data in the case of profiling which leads to increased accuracy for individuals. Remove the terms "lengthy" and "too long" and refer to Article 5(1)(e) of the GDPR instead.**

### 1.6. Profiling Necessary for the Legitimate Interests

***(See WP29 Guidelines — p. 21 Article 6(1)(f) — necessary for the legitimate interests pursued by the controller or by a third party)***

The WP29 guidelines outline several factors that it considers particularly relevant to take into account when organisations carry out the balancing test for profiling based on legitimate interest. One factor is the level of detail of the profile. The WP29 should clarify that granularity of the segmentation, especially in the context of marketing, does not mean that the legitimate interest of the controller is automatically overridden by that of the data subject. All the elements of the balancing test need to be taken into account, including safeguards.

The likelihood of identification increases the importance of protective measures. The WP29 should clarify that should the selection criteria for communicating advertorial content, such as the example they provide of a "native English teacher in Paris", single out a person, this would be considered granular. Typically, marketers make use of a combination of many variables in specifying the audience they would like to reach. A combination of variables such as "household with a garden + income level above average + age 60 plus + high affinity with gardening + has a car + lives within 30km of one of our gardening centre's outlets" are most typical of selections used in the past 40 years, with the efforts of companies to reduce communication cost and annoyance to consumers who are not interested in the company's offerings. Audience selection is a trade-off between precision (how many criteria to be used for the campaign) and reach (how many persons will be selected using the criteria). However, it should be taken into account that in practice most marketing campaigns will require at least one thousand people to be selected to make sense. Online, typically a minimum audience size is set not only for the purpose of the data subject's right to data protection, but also for fulfilling the minimum order quota set by service providers of the digital economic system.

**Recommendation: Clarify that the granularity of the segmentation does not necessarily mean the legitimate interest of the controller is overridden automatically by the data subject. This is one factor to consider in the balancing test and must be measured alongside the risks of the likelihood of identification of an individual and safeguards provided by the controller, such as setting a minimum audience size.**

### 1.7. The Right to Object to Profiling

***(See WP29 Guidelines — p. 25 — Article 21 — Right to Object)***

The WP29 should clarify that Article 21(1) does not impose a different legitimate interest standard than Article 6(1)(f). The WP29 guidelines note that once a data subject exercises his or her right to object to profiling, the controller must interrupt (or avoid starting) the profiling process, unless it can demonstrate compelling legitimate interest grounds that override the interests or rights and freedoms of the data subject. Controllers "profiling" on the legitimate interest ground would have already conducted the necessary balancing test, under Article 6(1)(f), to demonstrate compelling legitimate interest grounds that override the data subject's interests; moreover, they reassess it regularly to ensure that the earlier established legitimate interests still prevail. Accordingly, Article 21(1) should only require that, in the face of an objection by an individual, the controller must demonstrate that the earlier risk analysis and balancing test was, in fact, correct.

**Recommendation: Clarify that Article 21(1) does not impose a different legitimate interest standard than Article 6(1)(f) and that in the face of an objection to profiling, the controller must only demonstrate that the controller's earlier legitimate interest analysis was correct and that its legitimate interests still prevail.**

### 1.8. Profiling Flowchart

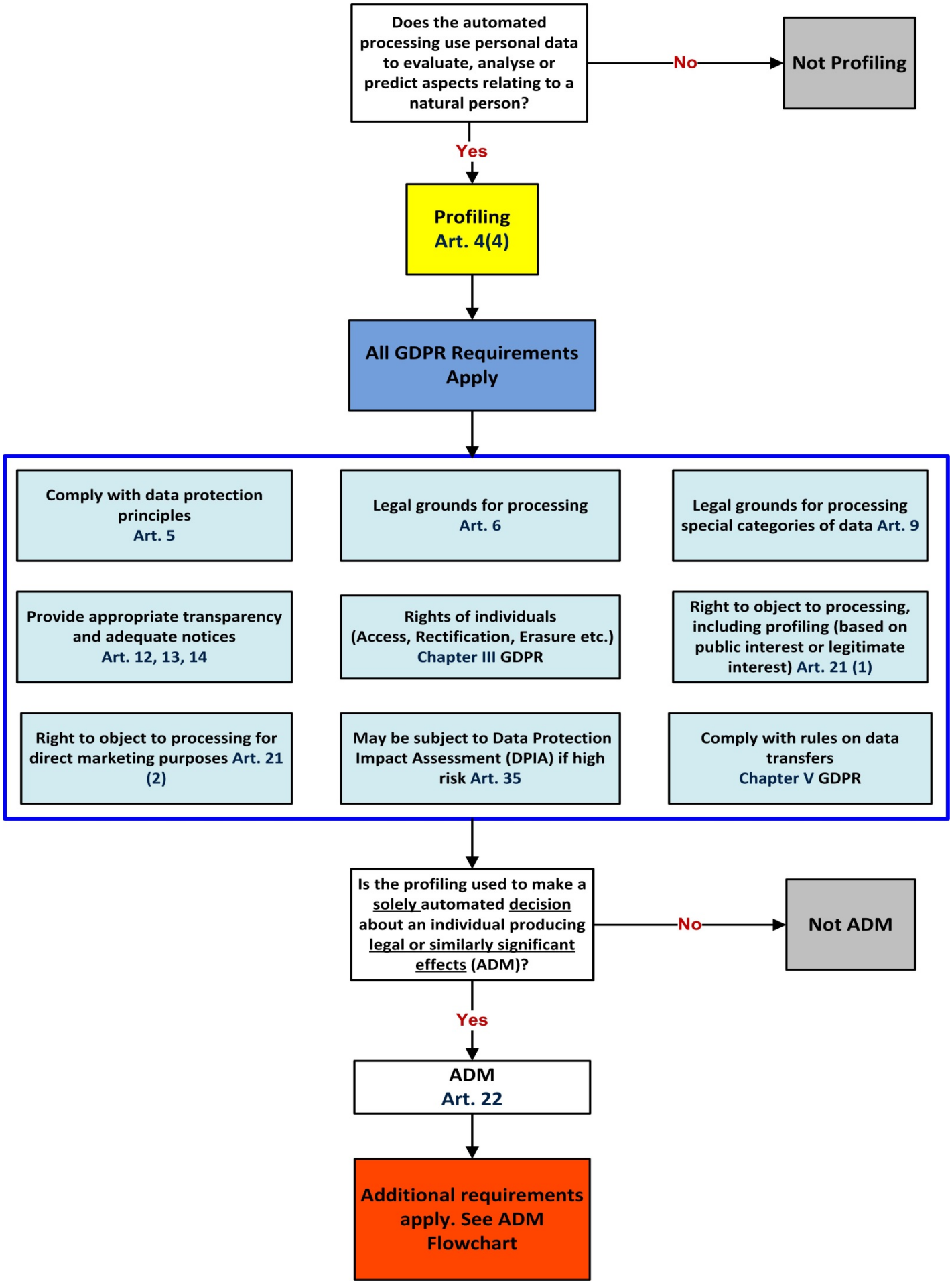
CIPL has prepared a flowchart to demonstrate, at a glance, the compliance requirements applicable to profiling under the GDPR. A similar flowchart could be included in the revised WP29 guidelines.

**Recommendation: Include a visual flowchart to assist companies in identifying the requirements of profiling under the GDPR.**

Centre for Information Policy Leadership
Hunton & Williams LLP

1 December 2017

# GDPR Profiling Flowchart



## Conclusion

CIPL is grateful for the opportunity to provide further comments on key implementation questions regarding profiling and automated decision-making under the GDPR. We look forward to providing further input on profiling and ADM in the future as new issues arise, particularly in light of any practical experiences in applying the GDPR.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.

# ANNEX

## Targeted Advertising and Article 22 of the GDPR

While targeted advertising has generated much discussion among privacy advocates and regulators, an optimal solution has not been found to balance data privacy with advertising objectives. CIPL believes that Article 22 of the GDPR is not the appropriate mechanism to address this issue. Its legislative rationale is different and meant to tackle decisions that create legal effects or similarly significant effects. CIPL believes that ADM, used in common and accepted practices of targeted advertising, does not produce such decisions. It is not clear if and what type of ads produce such effects, and CIPL believes that such a determination goes beyond data protection law compliance alone and should be subject to further discussion among experts from the advertising and consumer protection industries, behavioural economists and psychologists, privacy experts and other professionals. Finally, even after an industry consensus is reached as to what type of ads might fall under this category, CIPL believes each ad should still be looked at on a case-by-case basis, with only the most extreme instances of targeted advertising meeting the threshold.[20]

CIPL welcomes and agrees with the WP29's acknowledgement that targeted advertising typically does not produce similarly significant effects on an individual. While the WP29 also suggests that "it is possible" that some targeted advertising may produce such effects, CIPL does not agree with the example presented in the guidelines to demonstrate this (i.e. someone in financial difficulties who is regularly shown online gambling ads and is induced into generating further debt) and recommends that the WP29 consider removing this example. The example raises the following difficulties:

- It is impossible for organisations to know the likelihood of whether their ad will have a significant impact on someone, especially without collecting and analysing additional information. Forcing organisations to make such determinations may compel the collection of more information.

- Most targeted advertising is conducted on an "interest-based" model whereby an individual is assigned to certain ad categories that correlate with his or her online activities. Such categories are often generic and do not reveal specific vulnerabilities of individuals (i.e. that someone may be in financial difficulties).

- If a controller obtained actual knowledge of an individual's vulnerabilities and attempted to target ads at the specific individual to exploit the vulnerability, such a practice (which would be extremely rare and outside the practice of normal advertising) would be caught by the risk-based approach of the GDPR. It would require an advertiser to weigh the risks and harms of such a processing operation

[20] In such cases, if after an appropriate risk assessment is carried out and the benefits of the targeting outweigh the risks, then the ad may still potentially be shown to an individual under Article 22(2)(a)(performance of a contract) in scenarios where accepting advertisement is a necessary part of the business model that enables delivery of a service.

against the benefits. In such cases, the advertiser would be required to stop the processing and not proceed with the targeted advertising.[21]

In light of these issues, CIPL recommends the WP29 takes the following points into account:

1. **Human ad monitoring is impossible**: Save for formally protected categories of people and sensitive data, it is impossible and unrealistic to have a human monitoring and making decisions about which types of ads could be viewed as sensitive to an individual and ultimately cause a significant effect on them. Billions of ads are displayed to Internet users daily, and reviewing which ones may impact a particular user is unachievable. Moreover, prohibiting ads targeting certain classes of people can be problematic in that this may deny them an important benefit or a service.

2. **Algorithms can analyse signals for harmful personalisation**: Algorithms can be trained to automatically exclude delivery of certain ads based on profiles and would likely be more accurate at doing so than a human. Thus, companies might consider whether certain targeted groups are particularly vulnerable to a given product or service in a way that may raise legitimate questions of fairness and decency and ensure that their profiling processes do not target such groups.

3. **Non-targeted ads do not provide more protection**: Even without targeted advertising, the same ads may still reach the same consumer through generalised, non-targeted advertising. Where targeted advertising could, in fact, prevent the delivery of a certain ad, generic advertising may result in a consumer seeing a certain ad and thus it is not clear that not targeting certain ads resolves any underlying issues with respect to marketing any type of product to any vulnerable person. Additionally, how would this work regarding marketing a product to a person who should not spend any money on unnecessary (but otherwise non-nefarious) items because his or her limited resources are needed to support his or her family? There is no practical solution to stop showing this individual ads (either generic or targeted), and any ad may invite him or her to expend resources on new products or services.

4. **Users can opt out of targeted advertising**: Ad management, user transparency and empowerment regarding targeted advertising have become important issues for organisations and ad networks. In fact, all major Internet browsers today offer an option to manage targeted ads. Additionally, major online services offer ad managers which allow Internet users to remove interest categories from their profile, and targeted ads will reflect

[21] Also, it is questionable whether specifically targeting people to exploit their vulnerabilities would not involve the decisional participation of a human. For a controller to have actual knowledge of these vulnerabilities it would have to take measures to obtain this data, as ad interest categories alone are unlikely to reveal this (e.g. buying lists of individuals in financial difficulties through data brokers). Such affirmative action involves the controller in the decision-making process to specifically target these individuals with certain ads and arguably brings this type of activity out of the realm of solely automated processing for the purposes of Article 22 of the GDPR.

these preferences. Individuals who do not wish to receive any targeted ads can opt out of targeted advertising and remove themselves from all ad categories.

CIPL further recommends that the WP29 amend the four factors it presents as criteria to consider in determining whether an ad produces similarly significant effects, in order to create a more pragmatic approach. The factors as they stand will create further confusion and a lack of legal certainty among controllers. They may completely diminish the benefits of targeted advertising for individuals and lead to substantially negative impacts for advertisers for the following reasons:

- **The intrusiveness of the profiling process**: Intrusiveness is a broad and subjective notion. Profiling practices that are outside the remit of normal and commonly accepted advertising practices may be considered as too intrusive depending on context. Nevertheless, such practices would undergo a risk assessment to balance the benefits and harms of such processing.

- **The expectations and wishes of individuals concerned**: CIPL questions how this criterion would be implemented in practice. The expectations and wishes of individuals are highly subjective and impossible to predict in the absence of some affirmative action on the part of the individual. Moreover, many online services provide ad management tools for individuals to remove themselves from ad categories, to add new categories to their profile or to turn off targeted ads completely. These tools empower individuals to manage their own wishes and expectations for targeted ads.

- **The way the advert is delivered**: This criterion is overly broad as ad delivery can take numerous forms (e.g. pop-ups or ad displays on the side of a browser window). On one end of the spectrum, ads delivered through deceptive means, are illegal and/or would not survive a risk assessment, as required by the GDPR. However, normal and commonly accepted ad delivery methods do not rise to a level of producing a similarly significant effect.

- **The particular vulnerabilities of the data subjects targeted**: As outlined above, it is impossible for advertisers to know in advance whether an individual is particularly vulnerable to certain ads without collecting a great deal of additional information about the individual.

Regarding children, the WP29 guidelines note that because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes (see page 26 of the guidelines). The guidelines cite to a study on marketing to children between the ages of 6 and 12. However, as written, the guidelines could be interpreted more broadly to apply the study's findings to anyone under 18. This implies that, irrespective of whether consent is obtained from a child in line with Article 8 of the GDPR, anyone under 18 would be prevented from lawfully consenting to personalised advertising. Such an approach would be inconsistent with the GDPR's existing protections for children, where children of 16 years (or from 13-16, depending on the member state)

are deemed mature enough to give consent to the processing of their personal data without parental authorisation. Furthermore, the position is out of step, given that a 16 year old in many member states can lawfully consent to sex, marriage or surgical treatment, or join the armed forces. In addition, such a position would have a significantly negative impact on digital advertising for publishers and frustrate the ability of advertisers to reach young, independent consumers. Therefore, the WP29 should clarify that children who have consented to targeted advertising under the GDPR should not be prohibited from receiving personalised ads, as there is a valid legal basis for processing.

**Recommendation: Remove the example put forward to demonstrate a targeted ad producing a similarly significant effect (i.e. someone in financial difficulties who is regularly shown online gambling ads and is induced into generating further debt). Amend the four factors to consider in determining whether an ad produces a similarly significant effect, in order to create a more pragmatic approach. Clarify that children who have provided valid consent under the GDPR to targeted advertising can receive personalised ads.**