November 2017

Profiling, automated decision-making and breach reporting — Draft Article 29 Working Party Guidelines

BSA comments

BSA | The Software Alliance[1] (BSA) welcomes the opportunity to provide comments to the Article 29 Working Party on its recent draft guidelines concerning (1) automated decision-making ("ADM"); and (2) reporting of personal data breaches. The guidelines provided by the Article 29 Working Party will play an important role in clarifying the obligations of organizations across the digital economy. With that in mind, we endorse guidance that protects the data subject and also maximizes the ability of innovative firms to process data in ways that benefit users and society at large.

Profiling and Automated Decision-Making (ADM)

We welcome the draft's recognition that there are substantial benefits to profiling and ADM. The GDPR also recognizes and seeks to preserve these benefits, and for that reason adopts a balanced approach to regulating these activities — allowing, for example, profiling to be based on the "legitimate interests" legal ground and also differentiating in Article 22 between decisions that are fully-automated and "produce legal effects [on,] or similarly affect" data subjects, and all other automated decision-making. It is important that the Article 29 Working Party's guidelines fully reflect this legislative balance. To ensure that it does so, we believe the final draft merits greater consideration of the following points:

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the internationals marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*

BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Intuit, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Tend Micro, Trimble Solutions Corporation, and Workday.

1. **Article 22 provides a *right* not to be subject to certain decisions based on automated processing. The draft guidelines should not interpret it as a *prohibition* against those decisions**

GDPR Article 22(1) states that "*The data subject shall have the right* not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" (emphasis added). Article 22(2) then sets out three cases where this right is expressly set aside; for example because it would be inappropriate for individuals to be given the right not to be subject to legally-required anti-fraud monitoring, provided the law has safeguards, such as an appeal mechanism (see Recital 71).

The other rights, including the right to object in Article 21, the right to restriction of processing in Article 18, and the right to erasure under Article 17, are conferred on individuals in the same way. The GDPR does not presume that all individuals will, as a matter of course, want to block processing. Rather than adopting blanket prohibitions/obligations, this Part of the GDPR gives individuals *rights* — i.e., controls.

Yet when it comes to Article 22, the draft guidelines depart from the legislation. The draft presents Article 22 as a "*prohibition"* (see, e.g., pages 9, 15 and 31). Thus instead of the data subject having to actively object to the ADM, the controller can *only* undertake it — for any data subject — pursuant to one of the exceptions in Article 22(2).

The draft guidelines should be amended to accurately reflect the law. The GDPR is clear when conduct is prohibited (see for example Article 9(1)); this is not the case with ADM, however. Treating ADM as prohibited is also neither necessary nor proportionate: prohibition might be suitable if there was conclusive evidence that ADM is *per se* more problematic than human decisions. Instead, ADM only presents risks worthy of extra data subject control (i.e., rights) and transparency (Article 14(2)(g)/15(1)(h)), but *not* a prohibition that applies even when data subjects have no concerns. Moreover, any ADM is in any case subject to the full range of general GDPR protections, e.g., fairness, proportionality, privacy by design, accuracy, security, accountability, data subject rights, and enforcement by both data protection authorities (DPAs) and the judicial system.

Also, at p16, the guidelines suggest that Article 22(4) — which prevents certain ADM processes from using sensitive data, e.g. health data — applies to all ADM decisions. However, on closer examination of Article 22(4), it is clear that the legislator intended it to apply only to decisions to which Article 22*(2)* applies. In other words, the extra prohibition in Article 22(4) does not apply if data subjects have the benefit of the Article 22(1) right not to be subject to ADM. This is because extra protection under Article 22(4) is only required when the Article 22(1) right is suspended by Article 22(2). Of course, even in the absence of Article 22(4)'s compensatory protection, ADM would still need to respect the GDPR's fundamental rules on using special category data, for example the Article 9 prohibition (with exceptions) on use of such data, and purpose limitation. In addition, the text at p21 is confusing as the heading "necessary to protect vital interests," refers to vital interests while the body of the text references both "public interest grounds" and "vital interests." Article 9(2)(g) of the GDPR permits processing of health data as necessary for reasons of "substantial public interest," so the reference to Article 9(2)(c) at the end of Section III.B.4 is too narrow, and should be replaced by a reference to: "Article 9 and, in particular, Article 9(2)(c) or Article 9(2)(g)."

2. The guidelines should take a more restrictive approach to **determining whether a decision has "legal effects" or "similarly significantly affects"** the data subject.

The concept of "legal effects" and "similarly significantly affect" are pivotal to the legislative balance struck by Article 22. A decision should only be considered to produce such effects if it self-evidently forces a change of the data subject's situation or actively denies them something to which they are entitled.

For the most part, the draft guidelines (at p10-11) accurately reflect that distinction. However, at p11, and again at p26, they seem to suggest that merely influencing an individual's choices or behaviour would amount to effects that are "similar" to a legal effect, and thus potentially subject to Article 22. The draft guidelines give the example of advertising on-line gambling services to vulnerable individuals.

If a data subject has simply had their choices influenced, they are still the relevant decision-maker in respect of the *actually* significant effects envisaged here: whether to use the service. The process in question neither gives nor denies them anything significant. Thus it does not obviously fall within the drafting of Article 22. It is also clear from the examples given in Recital 71 that the effects the legislator had in mind (e.g. denial of job applications) is substantially more significant than "influence of conduct".

The draft guidelines, at p11, also suggests that differential pricing (using ADM) could be seen as producing an effect that is "similarly significant" to a legal effect, since "prohibitively high prices effectively bar someone from certain goods or services". But cost competition is an argument for *more effective* differential pricing, not against it (because differential pricing is designed to optimize pricing to make sure many customers can afford what is offered). Further, an individual's (in)ability to finance something is not usually known to the person engaging in the ADM; many people will not pay, just because they do not consider it to be good value for money (rather than being faced with an actual "bar"). The draft's suggestion that use of differential pricing strategies might violate Article 22 therefore seems at best unworkable, and potentially contrary to the Charter of Fundamental Rights (Article 16 — freedom to conduct a business).

Furthermore, one of the listed examples of decisions with "legal effects" provided at p10 detracts from the clarity the remaining examples offer. Specifically, the example of "automatically disconnect[ing a user] from their mobile phone service for breach of contract because they forgot to pay their bill before going on holiday" trivializes the concept of a "legal effect," and does not fit with the other facially significant examples of "legal effects" listed, e.g., denial of social benefits, or preventing border entry. It should be omitted from the final guidance.

In addition, the Article 29 Working Party should delete its cross-reference to the "substantially affects" language from their guidelines at p11 for identifying the lead supervisory authority because it's irrelevant to the interpretation of Article 22. The words are different ("substantially" vs. "significantly"), the context is different, and the purposes are different. The cross-reference, which includes an overly broad list of "helpful" examples, undermines the Article 29 Working Party's earlier statement at p10 that "the effects of processing must be more than trivial and must be sufficiently great or important to be worthy of attention."

Finally, there is also no obvious basis in the GDPR why Article 22 should be interpreted to also include a prohibition on ADM that has *positive* effects for individuals. Attempting to confer protection even when no negative effects are envisaged, does not seem rational or proportionate.

3. Article 22 should apply only to decisions based on evaluation of the characteristics **of the individual in question**.

At p12, the draft suggests that ADM can be caught by Article 22 even when the decision is based only on data about other individuals, not the person affected by the decision. It gives the example of setting people's credit limits based on similar individuals living in the area. This seems plainly contrary to Recital 71, which defines ADM as being a decision about a person "evaluating personal aspects relating *to him or her*" (emphasis added). It would also mean, effectively, that the controller processing personal data about the other individuals would need to consider legality of that processing based not just on the impact on the data subjects, but also another (potentially unknown) third parties (the eventual subjects of the ADM). This would be a fundamental departure from the GDPR's data subject-centric approach, which should have been subject to extensive impact assessment and democratic deliberation.

4. Guidelines should recognize that **audit and evaluation of ADM algorithms are legitimate secondary uses of personal data**

At p17, the guidelines recommend that "Controllers should carry out frequent assessments on the data sets they process to check for any bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations. Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling are other useful measures."

Usually, that audit will involve the processing of personal data - for example, looking back over past decisions to improve and enhance a model's accuracy, or using sample datasets to test the result for bias. As part of encouraging ADM audits, the guidelines should explicitly recognise that such uses are in principle a compatible further use of the data and that no further legal basis is required for such uses of data (per Recital 50). Other GDPR requirements in relation to such use — e.g. transparency, accountability and proportionality — would of course continue to apply.

5. **The GDPR does not prohibit asking for consent as a precondition to granting access to services**.

At p20, the draft says that "Where the data subject has no choice, for example, in situations where consent to profiling is a precondition of accessing the controller's services consent is not an appropriate basis for the processing".

It is unfair to say that someone has "no choice" in such a context — they can of course choose not to use the service, unless it is somehow a necessity. Even if the service *is* essential, such as mandatory health insurance, the data subject may have a genuine and free choice of plan (some of which require consent, and some which do not).

The draft's categorical position should also be revised in order to be more faithful to the drafting of the GDPR. Article 7(4) only requires "utmost account" to be taken of whether (among other factors) the provision of a service is conditioned on receipt of the requested consent.

Data Breach Notification

The breach notification regime introduced by the GDPR will help to drive improved data security practices. We strongly agree with the draft guidance, at p4, that the "focus of any breach response plan should be on protecting individuals and their personal data." Consistent with that objective, we recommend the following improvements to the draft guidelines:

1. **Deeming a controller to have knowledge of its processors' breaches** is inconsistent with data security technical and management realities

We agree with the draft, at p9, that a controller should be regarded as having become "aware" of a data breach when that controller has "a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." However, contrary to p11 of the draft, simply because controllers may use processors to achieve their purposes does not mean that those controllers are, therefore, "aware" of a breach once the processor has become aware — irrespective of whether the processor has notified the controller and whether the controller can with "a reasonable degree of certainty" conclude a breach has occurred.

A rule of this sort penalizes controllers who choose to use processors, by making the breach notification requirements for those controllers more stringent (and in some cases impossible to comply with). Given that processors are often better positioned than controllers to apply robust technical and organizational security measures to data, discouraging controllers from using processors seems inconsistent with the Working Party's goal of furthering data protection and data security.

2. Processors should be afforded **sufficient time** to investigate and assess

The GDPR does not mandate a time period within which a processor must notify a controller of a breach, except that it must do so "without undue delay." We understand the draft's recommendation, at p11, that processors notify controllers of a breach immediately, with further information about the breach provided in phases as information becomes available. We agree that timely notification from the processor to the controller is important in order to ensure prompt notification (where required) of DPAs and data subjects. However, we invite the Working Party to clarify that this does not exclude reasonable time taken by the processor to assess whether a breach has indeed occurred, and to determine which controller(s) need to be notified.

3. Emphasis that **notification** is **only** required where a data breach is **likely to result in a risk of adverse effects**

Article 34 is designed to mitigate the potentially harmful consequences to data subjects of a breach. Because the likelihood of harm to the data subject is the principle which underpins the notification guidelines, the test is therefore one of degree. That said, the draft guidelines are relatively unequivocal in parts about the circumstances in which notification to a DPA and/or communication to a data subject is or is not required. We invite the Article 29 Working Party to consider qualifying instances where it prescribes notification. The draft guidelines suggest that loss of personal data by itself triggers a notification and/or communication obligation. For example, at p15, the draft guidelines state that "communication to data subjects *would be required*, even if the data itself was subject to adequate encryption measures" (emphasis added). This cannot be taken as a rule. Instead, even in the context of an availability breach, what is important is the likelihood of the breach adversely affecting data subjects. We welcome this clarification throughout the guidelines, including in the annex (e.g., example viii, at p29, suggests that the unavailability of medical records in a hospital requires the notification to the DPA and communication to the data subject, without suggesting there should be an analysis of the likelihood of adverse effects).

Furthermore, at p19, the draft guidelines mention that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated. It is not reasonable to expect controllers to re-evaluate this for indefinite duration. We would appreciate if it could be clarified after expiration of which maximum period of time the controller's obligation to re-evaluate would cease to exist.

4. **Notification** to **lead DPA** in cross-border contexts

We welcome the draft guidelines reiterating the role of the lead DPA as "sole interlocutor" (GDPR Article 56(6)) in the context of a data breach — namely, by clarifying, at p15, that "whenever a breach affects the personal data of individuals in more than one Member State and notification is required, the controller will need to notify the lead supervisory authority." The guidelines, still at p15, suggest that controllers *may* notify other DPAs that are not its lead DPA but that notification of only the lead DPA will be sufficient if the controller indicates whether the breach involves other Member States.

We invite the Article 29 Working Party to ensure this position is reflected throughout the guidelines, including the annex. For example, in the annex, at p26, the draft guidelines suggest that *each* DPA must be notified where there is a cross-border effect: "*If the breach affects the individuals in more than one Member State, notify each competent supervisory authority accordingly*."

5. **Double fining** for a failure to notify or communicate a breach and the absence of adequate security measures is **contrary to the GDPR**

GDPR Article 83(3) clearly states that where, "for the same or linked processing operations," a controller (or processor) "infringes several provisions of [the GDPR], the total amount of the administrative fine shall not exceed the amount specific for the gravest infringement." In other words, a controller can be fined only once for multiple infringements relating to the same or linked processing activities, rather than being fined multiple times. To do otherwise would be overly punitive, as well as inconsistent with GDPR Article 83(1), which states that fines should be "effective, *proportionate* and dissuasive" (emphasis added).

In spite of this, the draft guidelines envisage a double fining framework for data breaches. At p8, the draft explains that DPAs may fine a controller once for a failure to notify or communicate the breach (under Articles 33 and 34) and once *again* for an absence of (adequate) security measures that led to the breach (Article 32). This approach risks leading potentially to fines that are several multiples of the sanctions foreseen in the GDPR and be not simply dissuasive as the legislator intends them to be, but even particularly disproportionate. As this would be inconsistent with Articles 83(1) and (3), we invite the Article 29 Working Party to revisit this position to better reflect Articles 83(1) and (3).

* * *

For further information, please contact:

Thomas Boué, Director General, Policy – EMEA

thomasb@bsa.org or +32.2.274.13.15