10

EUROPE
TechAmerica

THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

Comments on a Risk-Based Approach to Data Protection

Brussels, 03 May 2013

This paper has been put together following the 7-8 March meeting of home affairs and justice ministers, which discussed the possibility of "injecting a more-risk-based approach" into the draft Data Protection Regulation. It builds on both the work of the DAPIX working group to date, and the Opinions adopted by the various committees of the European Parliament. Please contact [redacted] for more details.

TechAmerica Europe represents leading European high-tech operations with US parentage. *Collectively we invest Euro 100 bn in Europe and employ approximately 500,000 Europeans. TechAmerica Europe Member companies are active throughout the high-technology spectrum, from software, semiconductors and computers to Internet technology, advanced electronics and telecommunications systems and services.*

Introduction

TAE welcomes the opportunity to comment on the development of a sound risk-based approach to data protection. Far from implying a reduction in effective levels of data protection, a risk-based approach has the potential to substantially improve outcomes for data subjects while reducing administrative burdens for data controllers.

A risk-based approach (which calibrates controls and supervision according to likely outcomes of data processing) should be contrasted with a *precautionary approach* (which seeks to minimise the possibility of any negative outcomes via strict ex-ante controls, and works on the basis of exceptions to a generalised prohibition on data processing) and also from a *harm-based approach* (which seeks to allow data processing until certain thresholds of negative outcomes are reached). Each of these implies trade-offs in terms of control, flexibility, innovation and substantive outcomes for data subjects and data controllers. Elements of all three approaches might be needed to create the optimal outcome in a European context

As a general observation, the proposal tabled by the European Commission adopted a largely precautionary approach to data protection. The main criticism of this approach has been that it led to overly-prescriptive provisions which actually reduce rather than increase legal certainty and administrative burden. Many have also commented that the move from the more principles-based 1995 Directive to the stricter compliance-based approach does not necessarily increase the likelihood of good data protection outcomes for data subjects.

The search is on, therefore, for meaningful changes which maintain the protections intended by the drafters, while allowing additional flexibility in the way data is processed and legal certainty for all parties. TAE engages in this discussion in a constructive spirit aimed at striking the right balance between protection and flexibility, control and accountability, to equip the EU with a framework that will remain valid for many years hence.

Contents

Definition of Personal Data and Data Subject

A workable definition of personal data is critical, since it defines the scope of the Regulation and the obligations and rights of data subjects and data controllers. Too broad, and data with only hypothetical privacy relevance or impact is subjected to disproportionate protection, with all the accompanying inconvenience and costs that this implies for consumers, data controllers and their processors; too narrow a definition, and a data subject's rights would not be adequately protected. This concept is ripe for the injection of a risk-based approach.

While the definition proposed by the European Commission largely repeats concepts which exist within the existing Directive (reasonableness test, ability to identify, direct and indirect identification) it *does* increase uncertainty on the status of an extended range of identifiers which may or may not, depending on the circumstances, be personal data. This has been done, inter alia, to respond to ECJ jurisprudence, e.g. Sabam v Scarlet which states that for example IP addresses are "protected personal data", albeit referring only to the specific context of a data controller allocating that IP address to a known subscriber.

TAE members agree that such identifiers are worthy of protection and are rightly in scope for the Regulation. However we believe the Regulation needs to provide more efficient mechanisms for distinguishing between all types of personal data across the entire spectrum from clear direct identifiers to data which can only hypothetically or with a significant effort and cost be linked to a data subject. The introduction of pseudonymous data as a subset of personal data would allow for an injection of a risk-based approach where it is most needed, and in a way which is entirely consistent with ECJ jurisprudence and the EU principles of necessity and proportionality. Failure to do so would leave data controllers confronted with the lack of legal certainty of Recital 24.

Pseudonymous data is a particularly helpful concept since it covers a range of business models, both offline and online, and so can have general application. It covers both data that were once personal and have had identifiers removed (for example for medical research), and data which has never been linked to any data subject, but where the possibility of identification nonetheless remains (such as web browsing data).

Pseudonymous data is data that is subject to controls that ensure that it is not used to identify a data subject.

- Technical – data should be separated or altered if applicable in such a way as to prevent the merging with other data which could lead to the identification of a data subject
- Organisational – data should be subject to separate decision-making structures, such that no one group has the autonomy and ability to merge data and reverse sets in a way that could identify an individual
- Legal – where the parties are from separate organisations, technical and organisational controls, should be reinforced by legal arrangements and commitments between parties involved not to allow data sets to merge in such a way that data can identify an individual without the data controller seeking an appropriate legal basis.

Furthermore, because pseudonymous data is a kind of personal data and within scope of the Regulation it should still be subject to the provisions of the Regulation; However, due to the specific nature of pseudonymous data and in particular the very thin personal layer embedded in it and the controls it is subject to it should be possible, under a risk-based approach, to consider certain alleviations for the processing of pseudonymous data. EP Rapporteur Albrecht himself acknowledged this possibility, without actually developing the concept further. Pseudonymous data should therefore be seen as an example of privacy-by-design and an example of the data minimization principle at work.

Logically, since the aim of pseudonymous data is to prevent identification of a data subject, the main mitigation could be to adapt the obligations under article 14 and waive the data subject rights outlined in Articles 15 to 18, since exercise of these rights requires the controller to have identified a data subject, and without such identification it is not feasible to offer these rights. Requiring a data subject to identify himself to avail himself of those rights is contrary to the data minimization principle. It could also create practical difficulties for data controllers that have developed systems designed to *not* identify data subjects if it were still possible for a data subject to identify themselves to a data controller and attempt to exercise their rights. In reality, this approach is already recognized in Article 10 of the Commission's proposal. Nevertheless, the proposed construction of a subset category of personal data (pseudonymous data) better reflects the risk based approach notion and brings more legal certainty.

Consistent with the idea that pseudonymous data can prevent identification of individuals, it should be legally permissible to process pseudonymous data **on the basis of the controller's legitimate interest**, and subject to the data subject's right to object under Article 19. Requiring other legal bases for pseudonymous data, particularly consent, is likely to be counter-productive since the requirement for explicit consent could lead a data controller to conclude that he needs to identify the individual more than at present. For example, if controllers are required to obtain explicit consent when utilizing a randomly generated cookie identifier (e.g. to optimize online services by using website analytics) then they would need to associate consent with a more consistent identifier than a cookie identifier (which can be deleted). Controllers would be likely to default to using email address or some other persistent identifier, with the result that they will collect more information than they would need to at present. Further comments on the use of the legitimate interest legal base follows below under the section on Consent.

<< Back to top

Profiling

The ability to process data to extract new actionable insights is absolutely essential to a knowledge-based economy, a key to building the information society, and therefore it is at the heart of the EU Digital Agenda. A risk-based approach needs to effectively protect the data subject whilst allowing legitimate and beneficial business activities that use advanced data processing techniques to continue and contribute to growth, jobs, entrepreneurship, innovation and competitiveness in Europe.

Article 20 extends the list of aspects identified in the current Directive which, when evaluated automatically, would constitute profiling to include the analysis of behaviour, personal preferences and location. However, the legal threshold beyond which the processing is to be prohibited (i.e "significant effect") is the same one as in the current Directive. This threshold now looks exceedingly vague given the much wider range of data processing activities to which it is to be applied. This dramatically increases the likelihood that a number of legitimate data processing practices could, over time, be considered by a supervisory body to cross the "significant effect" threshold. If the threshold is to be interpreted too strictly by supervisory authorities then it could easily result in the prohibiting of many beneficial data processing techniques and enabling technologies across sectors. In some cases, for example, failure to use data (e.g. to diagnose a medical condition) can lead to bad outcomes – not only at an individual or societal level but also in economic terms, just as its use can create risks.

A risk-based approach therefore would move away from the underlying *precautionary* approach, which carries a risk that a many processing activities could capriciously be considered to have a "significant effect", by introducing a higher threshold of "***significant adverse effect",*** thus focusing regulatory supervision on the most risky kinds of data processing. Another good risk management technique would be to make clear that, where a decision has a significant effect on a data subject, that data subject has a right to obtain human review of the decision (provided, that is, that they can be identified). This reflects the intention of Article 15 of the current Directive which does not prohibit automated decisions, but rather seeks to ensure that human intervention is possible.

Even where data processing has a significant adverse effect, it should be allowed whenever it is legal, i.e. wherever there is a legitimate legal base, since all legal bases include safeguards and balancing checks for the interest of the data subject; or where only pseudonymous data is used, in order to incentivise the use of data that does not identify specific individuals; or where a provision in national law allows for such profiling.

On the other hand, and following the lead of the compromise reached in the JURI committee, profiling could be further restricted where it has the effect of discriminating against individuals on the basis of sensitive categories of data without prejudice to the provisions of Article 9.

[<< Back to top](#)

Consent

Consent is one of the three main legal bases for processing personal data available to commercial operators, along with contracts and legitimate interest. Improving the quality of user consent, where consent is used to validate processing, and achieving greater transparency over the processing of data in general, are both laudable objectives of the Regulation. However care must be taken to maintain the delicate balance between these legal bases.

The proposed Regulation[1] departs from the risk-based approach that was adopted in the current data protection Directive, which maintained a clear distinction between sensitive data and other personal data, and gave data controllers greater flexibility in determining how they would obtain consent.

Any supposed benefits in terms of legal clarity from a single standard for consent need to be balanced by the potential disruption caused by a change in the rules to business models with a lower privacy risk. A risk-based approach would maintain a distinction between different categories or contexts of data processing. In today's digitized world, implied or at least unambiguous consent should be deemed sufficient for ordinary processing of non-sensitive personal data. It has been argued extensively that it is at least more workable and less disruptive in the online world; but importantly, it is sufficient to protect data subjects when the processing does not present specific risks for those data subjects.

A higher level of consent may be necessary in order to minimize doubts as to whether individuals have agreed to their personal data being processed in a particular way that presents specific risks. Maintaining the risk-based approach, the proposed Regulation should require explicit consent only for those processing operations that "present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes" as foreseen in Article 33.2.b) to e) and Article 20 (new)..

It is worth noting that the conditions under which a controller can assert their legitimate interest to process data are already subject to a balancing test with the rights of the data subject. This is a proportionate and risk-based approach which we support and we agree that it is important that legitimate interests is not abused in ways that can harm data subjects. However any amendments to the text, or the later addition of delegated acts, which tend to *further* restrict the availability of the legitimate interest legal base and drive data controllers towards having to obtain consent where they currently do not require to do so would form part of a more precautionary approach which could subject less risky processing to more onerous control than is merited. Importantly, it would also impact on the balance between data protection law and another fundamental right, the right to do business. The economic impact of such far-reaching changes to a critical mechanism of data protection law would need much greater analysis. *See also comments on legitimate interest in section above on pseudonymous data.*

[<< Back to top](#)

Data Protection Officers, Privacy impact assessments, and prior Consultation

[1] Regarding the quality of consent, the current draft of the Regulation appears to deviate from a risk-based approach to consent in two important ways:

- the word "explicit" has been added to the existing requirement that consent be specific and informed. Under the current Directive, "explicit" consent was reserved for the processing of special categories of data. The Commission, in effect, seeks to establish a single standard for consent for data processing in all conditions, without consideration of the risk.
- The explanation in Recital 25 that "silence or inactivity" should not constitute consent, together with the requirement for explicit consent, has been taken by some commentators to mean that the Commission has substantially restricted the conditions for obtaining consent compared to the current directive, and that implied consent will no longer be allowed.

Much discussion of the EC proposal has focused on aspects of the Regulation that might increase or reduce the compliance burden for data controllers in ways that are not consistent with any reasonable assessment of risk. Elements of the EC proposal adhere to a risk-based approach, while others do not. For example, mandating a DPO for a company just because they have more than 250 employees (Art 35(1)b) appears to fit under a precautionary approach, rather than a risk-based one. Deleting Art 35(1)b takes the size of the company out of the equation and focuses on the risks.

The approach to privacy impact assessments does, on the whole, follow a risk-based approach. PIAs are required where there are specific risks as defined in Article 33. Where a PIA highlights a ***high*** degree of ***specific*** risks (note the existence of two separate and cumulative factors) this would justify some form of prior consultation with a supervisory authority. There is, in other words, an escalation path that is triggered by the identification of more serious risks.

However, we believe that it is important that there is no automatic link between Article 33 (Data protection impact assessment) *and Article 34 (*Prior authorisation and prior consultation*)*. Much of the language used in these articles is similar, and the words highlighted above which trigger the more onerous obligations under Article 34 are not clearly signposted. This impression is underlined by the circular logic that links these two articles: if your processing has a *significant effect* on a data subject then it is considered risky processing and would require a PIA. For that reason it is difficult to imagine a PIA under Art 33(2)a that does *not* also automatically require prior consultation with a supervisory authority under Article 34. Unless it is made clearer that there is no automatic link between conducting a PIA under Article 33 and the requirement for prior authorization under Article 34, then PIAs are not part of a truly risk-based approach - aimed at encouraging data controllers to identify risks and put in place mitigations before they materealize. They are simply the documentation of already known risks (I know my processing is risky so I must conduct a PIA) and an additional bureaucratic step on the way to prior consultation. As currently drafted, the mere fact that you are conducting a PIA means that you are likely to need to seek prior consultation and possibly even authorisation.

Another factor is that DPAs retain a very broad power to unilaterally determine that certain types of processing are risky and require prior authorization. This appears to subvert the logic of PIAs as a risk management tool, undermines the autonomy of data controllers, and risks creating divergences in interpretation across the EU. Any automatic requirement for the prior authorization of a DPA should be removed on the grounds that this is an overly-bureaucratic element from a purely precautionary approach, or limited to very strict cases such as when a new technology is being deployed for the first time.

An alternative approach to the risk-based approach would be to adopt a harm-based approach. This would leave the decision whether to conduct a PIA, appoint a DPO, or consult with a DPA, at the discretion of a data controller. Data controllers would therefore take responsibility for the consequences of the decisions they take around data processing they undertake based on the appreciation they make of the potential harm. Should a harm occur, the controllers would be held accountable to the supervisory authorities. Under this model, the absence of these voluntary controls would constitute an aggravating factor in the event of a breach of the law which was deemed to require the imposition of a sanction.

Alternatively, and to leave the current architecture of the regulation more or less intact, another approach would be to try and define the kinds of *significant effects* that the regulation wants to prohibit. However, it is inherently difficult to define risk, or to develop a risk assessment framework that works well for all kinds of processing in all kinds of situations. For example, the Alvaro amendments to LIBE attempted this and succeeded only in defining a matrix that effectively would capture most data processing as risky.

<< Back to top

Data breach notifications

The risk-based approach has the potential to be well developed in the provisions on personal data breach. As Council considers the many aspects of these rules, some key conditions should apply in order to follow a risk-based approach:

- Notifications should not be subject to a specific hard deadline in Article 31 which would be unrealistic and even counterproductive. A specific deadline may not be workable in all circumstances, and could divert efforts from the actual investigation and remediation of a breach to the hasty completion of the administrative notification procedure. On the one hand, this could unhelpfully distract controllers from the most urgent effort which should be to mitigate any risk of harm to data subjects arising from the breach. On the other, precipitated notification before the incident can be properly investigated and assessed could itself increase such risks or create new ones.

- Notifications should only be triggered by breaches above a certain seriousness threshold, i.e. where the breach poses an effective risk, i.e. it is likely to have a serious adverse effect on the data subject. The harm threshold defined in article 32(1) of the Commission proposal (notification to the data subject) should also be introduced into article 31 (notification to the authority).
- Not apply if the breached data is protected by technological measures that make it unintelligible to any unauthorized person (i.e. where the breached data cannot be exploited and therefore there is no actual risk involved).

[<< Back to top](#)

Roles and responsibilities of Data Processors and Data Controllers

The current Directive adopts a risk-based approach to the relationship between a data controller and a data processor working on their behalf by clearly demarcating their roles and liabilities. The controller remains responsible to the data subject for the protection of the data subject's rights. The processor's main obligation is to securely protect the data they are instructed to process. The controller defines the conditions within which the data processor should work and passes on those obligations to the processor contractually, *according to the level of risk involved with each particular processing*.

The draft regulation would fundamentally change this concept – and inject confusion into well-settled contractual relations -- by establishing joint liability between all data controllers and data processors. The proposed Regulation therefore adopts a precautionary approach which seeks to extend obligations and liabilities as widely as possible allegedly to ensure maximum protection for the data subjects. However, where obligations are directly imposed on the processor by law (as opposed to by contract with a controller) the processor can no longer rely on the controller's instructions alone, and will thus have a need to "know" the data subject and the context of the data processing in which they are involved in order to understand their obligations to secure the data. Conversely though, because the controller is no longer fully and exclusively in charge of complying with the legal requirements on processing, its own ability to properly assess, understand and manage the risk involved in the processing is damaged. Last but not least, the risk to the privacy of the data subject is also increased, both because documentation and information requirements are duplicated in breach of the data minimisation principle, and because the data subject loses the certainty of having to deal with one single entity, the data controller, when seeking remedy. This blurring of lines between the two parties' roles in every case, without consideration of the context or risk, creates unnecessary compliance burdens, impinges on companies' freedom to contract, and is likely to confuse established consumer relationships.

For example, the documentation requirements may increase the administrative burden on organisations rather than lead to a reduction as envisaged by the European Commission in its proposal. It is unfortunate that there is no requirement to assess the risks of data processing when determining the administrative requirements applied to the data controller and processors in particular situations.

All together, these changes – based on a precautionary rather than the current risk-based approach – will oblige companies to invest in compliance with unnecessary precautionary instructions, potentially diverting resources away from innovation and value creation, with a corresponding impact on jobs and growth. It remains a source of on-going frustration to industry of all kinds that this issue is not well understood, and that the potential impacts of such a change to the status quo are routinely downplayed.

[<< Back to top](#)

Establishment, supervision and the consistency mechanism

Another key aspect of the risk-based approach relates to the concept of establishment and the conditions under which data controllers and data processors are supervised by national authorities. A situation whereby multiple supervisory bodies are able to assert jurisdiction over the same entity for the same data processing operations is inefficient and harks back to the legacy system which was based on national approaches to risk management. If correctly done, greater harmonization can dramatically reduce the compliance burdens for organizations and at the same time ensure a high level of protection for data subjects. This is especially important for enabling the European single market and for helping companies to operate in multiple Member States. As such, for the one stop shop principle to be effective, the Regulation must afford organizations, data protection authorities ("DPAs") and data subjects' greater legal certainty. The processes whereby European DPAs can co-operate and assist each other should also be improved.

Under a risk-based approach, the competence of a lead supervisory authority should be clear, to avoid unnecessary bureaucratic procedures that would jeopardize the legal certainty that the principle provides to organisations. Coordination between supervisory bodies should not cause unnecessary delays in the provision of redress to the data subject. As the EDPS has rightly stated in their opinion on the Commission's proposal, the consistency mechanism should therefore be seen as a measure of last resort used only in exceptional situations.

Where organisations not established in the EU are covered by the new Regulation and subject themselves to supervision by EU authorities through the appointment of a Representative, it is critical that they should have access to the consistency procedures on the same basis as organisations established in the EU. Appointment of a Representative clearly demonstrates the intention of such organisations to comply with the EC's risk management framework, so further discrimination with EU operators on the basis of location is not justified by any risk-based approach.

A more risk-based approach to supervision and consistency would therefore include:

- Elimination of any discrimination among covered organizations (whether EU based or not) in the application of the one-stop-shop principle.
- A more efficient consistency mechanism, limited to serious cases where the competent authority is unable to take appropriate measures within a reasonable timescale.
- Better safeguards for all interested parties and Council and the European Parliament in eliminating inconsistencies of interpretation.

<< Back to top

For further information please contact:

[redacted]
TechAmerica Europe
Rue de Namur 16
1000 Brussels
[redacted]