AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

AmCham EU Comments on the Working Party 29 guidelines on data Protection Impact Assessment (DPIA)

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

The American Chamber of Commerce to the European Union (AmCham EU) brings together U.S. companies investing in Europe from a broad range of sectors, including aviation, consumer goods, energy, financial, heavy industry, pharmaceuticals and technology, among others. AmCham EU members typically operate globally with a strong presence in Europe and the Unites States. As such, they may have multiple business units with various governance bodies in more than one jurisdiction, including primary decision-making functions outside of the EU.

When formulating guidance and rules on these and other issues, we encourage regulators to consult regularly and work closely with stakeholders, including industry. In order to support this process, AmCham EU adopted a position paper including recommendations for the data protection authorities (DPAs), the European Data Protection Board (EDPB), and Member States to consider as they develop guidance and policies on the GDPR.

We welcome the on-going consultation on the DPIA procedure and previously submitted comments to the draft guidelines on portability, DPOs and identification of the lead supervisory authority. AmCham EU calls on the WP 29 to formalise this process even more, notably by providing a timeline for a consultation, and organising open and regular consultations and reporting back on the comments received.

Preliminary comments

- The protections in the GDPR for "high risk processing," and the DPIA procedure, both have the potential to significantly benefit data subjects – but both also risk creating disproportionate administrative burdens if guidance about these measures lack pragmatism.
- A key concern of AmCham EU is that the rules in this areas are not clear, and could result in divergent interpretations across the EU, in particular if DPAs develop different criteria. Therefore, AmCham EU welcomes the publication of guidance on the DPIA requirement by the Working Party 29.
- As a first step additional context should be provided on what constitutes "high risk processing," for example through factors or criteria that data controllers can take into account when conducting their internal assessments. These criteria should be based on evidence that relevant processing activities carries a risk of serious harm to data subjects.
- In addition, when considering risk, DPAs should bear in mind that all processing, whether high risk or not, is subject under the GDPR to significant redress and supervision, heavy sanctions, and duties to put in place appropriate data protection measures and follow privacy by design and default principles. These protections limit the number of scenarios where there will be a genuine and proportionate need for the additional protections reserved for "high risk" situations, including the adoption of DPIAs.

Which processing operations are subject to a DPIA?

- DPIAs should be based on quality not quantity. This will ensure that DPIAs can focus on those situations where they will truly ensure that the standards of privacy are improved by its conduct. For example requiring a DPIA for any "large scale"-data processing effectively sets aside the risk-based approach in the GDPR. Any data processing operation could be large scale even if there are no actual risks to data subjects from the collection of data.
- A DPIA should not be based on the type of data being processed. Instead, as the text states, the requirement should be based on the nature, purpose and scope of the processing. Categorizations beyond those identified in Article 35(3)(b) (i.e., special categories of data in Article 9(1) or personal data relating to criminal convictions and offences in Article 10) go beyond the scope of the regulation. For example, the GDPR does not define electronic communications data, location data and financial data as, per se, special categories of data. As such, processing of such data should not, in the absence of other factors, require a DPIA. Similarly, processing of personal data as part of a service broadly available to data subjects should not require a DPIA simply because vulnerable data subjects such as children could access the service.
- As provided in Article 35(4)-(6), supervisory authorities should provide a consistent list of the kinds of processing operations for which a DPIA is required or not required. To support consistency, this list should be centralized so that controllers and processors can ensure they are aware of the determinations of all supervisory authorities. The guidance should make a clear reference to Article 64(1) GDPR which calls for the need of consistency among DPAs with respect to the adoption of list of processing operations subject to DPIA.
- The new guidance suggesting that meeting two criteria from the list of 10 triggers a DPIA requirement is arbitrary and should be changed. Risk to data subjects should be determined in a holistic manner—not based on an arbitrary formula of meeting a certain numerical threshold. For example, the proposed "two criteria" threshold means that companies that process large amounts of data and that rely on processing outside of the EU – either directly or because they rely on processors that include operations outside of the EU - will almost always need to conduct a DPIA for all processing. This is also the case even if the data is transferred on the basis of an adequacy decision under Article 45 or subject to other GDPR-approved transfer mechanisms. This is because one criterion is data transferred outside the EU, and a second is data processed on a large scale. Thus, the "two criteria" threshold based on the criteria identified by the Working Party 29, does not allow to make an effective assessment of the presence of a high risk.
- More specifically and with regard to the identified risk factors:

  High Risk Factor 1 on Evaluation and scoring (pages 7 and 8): The inclusion of this factor, which includes "a company building behavioural or marketing profiles based on usage or navigation on its website" is overly expansive when it is read in this context and should be limited. Factor 1 cites Recitals 71 and 91 as justification for its existence.

Profiling that does not lead to legal or similar effects and that does not involve sensitive data should not be *per se a factor* triggering the presence of a high risk. Recital 71 states that "the data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention." Thus Recital 71 requires fully automated processing plus a high risk of harm—either a legal effect or an effect that is similarly significant to a legal effect. This is reinforced later in the recital: "Such processing includes 'profiling' that consists of any form of automated processing of personal data . . . where it produces legal effects concerning him or her or similarly significantly affects him or her". Clearly the GDPR foresees the need for a significant risk of harm.

Furthermore, Recital 91 states that a DPIA should be carried out where "personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of sensitive special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures." Here, the profiling or processing is concerned with special categories of data that are inherently more sensitive if disclosed or misused. So again, as in Recital 71, the concept of high-risk processing is tied to an actual risky processing.

The **high-risk factors 2 and 4** appropriately capture the risk-based approach laid out in the GDPR and demonstrate that Factor 1, which is not risk based, is not necessary or appropriate. High-risk factor2 on automated-decision making with legal or similar significant effect (page 8) captures the risk of potentially significant impacts to the rights and freedoms of individuals specified in Recital 71. The fourth factor on sensitive data (pg. 8) captures the risk-based approach specified in Recital 91.

Similarly, **factor 5 on data processed on a large scale** (pages 8-9) should include a consideration for risk. Currently, it provides four quantitative aspects for consideration, including number of data subjects concerned, volume of data, duration or permanence of processing and geographical extent of the processing. Other risk factors should be included—for example, the relative sensitivity of the data or use of new technology. Looking at the "sensitivity" requirement, for instance, the capture of device information (such as the discharge rate of a battery) even for a very large number of people carries minimal risk compared to other processing activities. Therefore, to surpass the high risk threshold, an exceptionally large scale processing should be required.

High-risk factor 9 on data transfer across borders outside the European Union - taking into consideration references such as "envisaged country or countries of destination" and "the possibility of further transfers": The reference to recital 166 creates the wrong impression that international data transfers create a high risk and there is an obligation to perform a DPIA whenever there is an international data transfer. This was not the intention of the legislator. If a data controller complies with the provisions of Chapter 5 (e.g. the controller is relying on binding

corporate rules, standard contractual clauses, or a similar EU-approved data transfer mechanism), data transfer across borders should not be a criterion for determining "high risk".

- More guidance is needed in cases where the views of the data subject would not be considered as "appropriate" during the conduct of a DPIA – i.e. cases where the use of the data is related to an unreleased product or service where confidentiality and the protection of intellectual property are imperative. The term "where appropriate" should not be interpreted too broadly in order to avoid overburdening organizations. This is especially the case when the DPIA concerns a product that has not yet be publicly launched. It should also be recognised that there are many ways to seek the views of data subjects such as user studies, public seeds of software etc.
- The updated guidance should include consent in the assessment of the likelihood and severity of the risk. Where consent is provided in accordance with Article 7 of the GDPR, it should be considered as an indication that the individual is informed and has agreed to the contextual element around the data processing, including the risks involved. Therefore, consent should be taken into consideration when assessing the risks.

How to carry out a DPIA?

- The Working Party recommends that where a controller relies on a processor, roles and responsibilities must be contractually defined and the processor must assist with the DPIA (page 14). How this is addressed in the contract should depend on the context of the service the processor provides to the controller under the contract. For example, where the controller contracts for a generally available service, the DPIA should be consistent, standard and broadly available in the same format for all controllers contracting for the same service. In contrast, where the controller is contracting for a custom software or service, as in software or a service that is developed uniquely for that controller, the DPIA should reflect that bespoke offering.

  Sector-specific DPIAs should be limited to subject matter-based sectors (e.g., health care) vs. technology-based sectors (e.g., cloud, mobile, on-premises).
- AmCham EU welcomes that the WP 29 clarifies that publishing the DPIA is not a legal requirement. The updated guidelines should however state more clearly that the decision not to publish a DPIA will not be used directly or indirectly against the concerned organization. In some cases, the publication of a DPIA could be problematic because it could go against its purpose. If an organisation is detailing how it manages its risks, this could leave the information open to potential hackers who might know what to target. Related to this, if you only publish a 'lighter' version of your DPIA, it won't give the data protection bodies more confidence in how you have managed to fulfil this requirement of the GDPR. It could turn into a "tick the box" exercise with no added value. As the publication of a DPIA is only recommended in the GDPR, it needs to be ensured that there are no consequences for those who do not publish the DPIAs.
- More guidance is needed on prior consultation. The "prior consultation" process should also be approached pragmatically, and required only where strictly relevant. The GDPR is clear that prior consultation is only triggered when the data controller determines a particular type of processing qualifies as high risk, but is unable to mitigate these risks to data subjects. Before formally consulting DPAs as provided for by Article 36 GDPR, organizations should have the possibility to informally engage with DPAs.