DIGITALEUROPE

# DIGITALEUROPE's views on Article 29 Working Party draft Guidelines on Data Protection Impact Assessments (WP 248)

*Brussels*, 23 May 2017

## EXECUTIVE SUMMARY

DIGITALEUROPE, as the voice of the digital technology industry in Europe, welcomes the opportunity to comment on the Article 29 Working Party's ("WP29") draft guidelines on data protection impact assessments ("DPIAs") and how to determine 'high risk' processing (WP 248). DIGITALEUROPE believes that the effective implementation of the General Data Protection Regulation ("GDPR") will require a joint effort between all stakeholders **built on mutual trust**. We therefore welcome the decision of the WP29 to treat all guidance documents, including WP248, as a draft guidance document while encouraging feedback from the data protection community.

DIGITALEUROPE believes that the main objective of WP 248 should be to achieve **legal certainty** so that data controllers of all sizes across the EU clearly understand which processing operations are subject to a DPIA, how to carry out a DPIA, and when to consult the supervisory authority. While we welcome some of the clarifications presented in the draft document, we believe further clarifications would be helpful. DIGITALEUROPE has structured its comments in the following manner, aimed at summarising our key views:


- Section III A – What does a DPIA address
- Section III B.a.1 – Evaluation or Scoring
- Section III B.a.3 – Systematic Monitoring
- Section III B.a.4 – Sensitive Data
- Section III B.a.5 – Data Processed on a Large Scale
- Section III B.a.6 – Datasets that have been Matched or Combined
- Section III B.a.7 – Vulnerability
- Section III B.a.8 – Innovative use or applying Technological or Organisational Solutions
- Section III B.a.9 – Data Transfers outside of the EU
- Section III B.a.9 – Documentation
- Section III B.a.9 – Re-assessing DPIAs
- Section III C – Seeking the views of Data Subjects
- Section III C.d – Publishing of DPIAs



DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

## OVERALL VIEWS

DIGITALEUROPE welcomes the recognition of the WP29 that the notion of DPIAs and 'high risk' are context specific and that entities must have a level of flexibility to devise their specific risk assessment frameworks. Moreover, we welcome the initial thoughts put forth by the WP29 on framing the challenging debate of what constitutes 'high risk' data processing operations. DIGITALEUROPE is encouraged that the WP29 avoided the creation of a 'static' list of 'high risk' processing activities, as this would not stand the test of time and quickly become outdated.

However, DIGITALEUROPE is concerned that the approach taken in the draft guidelines will **result in organisations interpreting DPIAs as a mandatory exercise for the majority of data processing activities**. The GDPR has designed DPIAs as an 'exceptional instrument' to be used only in truly 'high risk' situations. The potential for the draft guidelines turning DPIAs into a mandatory activity does not reflect their envisaged purpose in the GDPR and will lead to increased administrative burden for both data controllers and data protection authorities ("DPAs").

While the draft guidelines focus closely on factors that may exist 'when a DPIA is required' we would encourage the WP29 to provide more concrete examples of 'high risk' processing, avoid guidance that falls outside of the scope of the requirements set forth in Article 35(3), and further provide instances of 'low risk' data processing when a DPIA is *not* required (noting those examples are non-exhaustive). This would bring additional clarity to data controllers and avoid unnecessary DPIA exercises. In doing so, the scarce resources of data controllers and DPAs could be focused on those situations where a DPIA will truly ensure that the standards of privacy are improved by the data controllers conduct. The focus on quality over quantity will ensure that where a DPIA is undertaken, it will meet the standard required by the GDPR.

## SPECIFIC CONCERNS

### 1. Section III A – What does a DPIA address

The draft guidelines note that along with the obligation of a data controller to carry out a DPIA when using a new technology product that '*is likely to be used by different data controllers to carry out different processing operations*', the data controllers may be 'informed' by a DPIA previously executed by the developer of the new technology product. DIGITALEUROPE wishes to inform the WP29 that in some instances the developers of the new technology are not considered as data controllers and as such are **under no obligation to perform a DPIA**. Such entities should not be obliged to execute a DPIA simply because they have created new technology, particularly when they are not acting as data controllers. It is the responsibility of the entity actually processing personal data to undertake a DPIA as it may be processing the data in ways simply not contemplated by the developer. DIGITALEUROPE does believe that where it is in a position to do so, the developer may assist by making available relevant information that would otherwise not be known to the data controller.

However, even in instances when the creator of the new technology does choose to complete a DPIA and provide it to the 'user' of the new technology, there are **risks of disclosing sensitive intellectual property and confidential business information**. Similar trade secrets and confidentiality concerns arise with respect to joint controller relationships, where the WP29 states joint controllers must 'precisely' define their roles with respect to the joint processing: "*When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects.*"

As such, we would welcome clarification from the WP29 that an entity acting as a processor may limit the information provided in such a DPIA to protect intellectual property and confidential business information and to avoid security risks. We would also welcome clarification that in the case of joint controller relationships, a joint controller may define its role with respect to the processing without revealing any confidential information such as trade secrets, intellectual property, or privileged information.

Additionally, DIGITALEUROPE is concerned that the notion of 'similar processing' is very narrowly defined by the WP29. Indeed, according to the draft guidance, "*This might mean where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA.*" We would like to draw the WP29's attention to the many possible instances where a data controller may implement similar features or run similar software across different products. In such cases, the processing for parts or all of the product may well be covered by an existing DPIA. This would also be the case for existing products released in multiple iterations or versions. In such instances, an existing DPIA could be relied on and updated or completed to address any new risks or processing.

We would welcome clarification that for new implementations of similar feature or software, even across different products or newer versions of existing products, controllers may rely on existing DPIAs for the similar feature or software used. 'Similar processing' need not pertain to the exact same product, but could pertain to a type of processing that is prevalent across multiple different products, and that covers part or all of a product.

## 2. Section III B.a.1 – Evaluation or Scoring

The 'evaluation or scoring' criterion proposed in the draft guidelines cites Recitals 71 and 91, but also exceeds their scope. Indeed, while Recital 71 addresses the evaluation of personal aspects such as 'personal preferences or interests, reliability or behaviour, location or movements', it is *only* insofar as this is used for decision-making that produces legal effects or similarly significantly affects the data subject. Recital 7 specifically identifies "***automatic refusal of an refusal of an online credit application or e-recruiting practices without any human intervention***" (emphasis added) as examples of automated decision making that would produce legal effects or similarly significant effect. Profiling that does not lead to legal or similar effects and that does not involve sensitive data should not be considered a 'high risk' trigger. However, behavioural or marketing profiles based on website navigation would not necessarily carry comparable risk. The mere existence of some form of evaluation or scoring should not suffice to fill one of the criteria for a DPIA.

DIGITALEUROPE believes this criterion should instead focus on the **intended use of the evaluation or scoring** and whether the processing will produce legal effects or significantly affect natural persons, and whether it will likely result in 'high risks' to the rights and freedoms of natural persons and not on the mere fact that such an evaluation will take place.

## 3. Section III B.a.3 – Systematic Monitoring

DIGITALEUROPE believes 'systematic monitoring of a publicly accessible area on a large scale' as identified in Article 35(3)(c) clearly applies only to the systematic monitoring of physical spaces (e.g. via CCTV), based on the language of the text. However, we believe the draft guidelines would benefit from further clarity and confirmation that 'monitoring' covers only physical monitoring (e.g. via CCTV). Also, in the case of CCTV, most DIGITALEUROPE members restrict CCTV to what is absolutely necessary for the protection of employees, customers and property

and any monitoring of public spaces is purely incidental to those objectives. It should be confirmed that such usage would not trigger a DPIA.

## 4. Section III B.a.4 – Sensitive Data

DIGITALEUROPE does not agree with the suggestion that the processing of 'sensitive data' in itself should be considered a criterion. The GDPR specifically mentions a higher threshold of 'processing on a large scale of special categories of data'. DIGITALEUROPE would encourage the WP29 to include this additional clarification into the final guidelines so that organisations do not incorrectly interpret that any processing of 'sensitive data', when not on a large scale, will count as 1 of 2 the criterion towards triggering a DPIA.

Moreover, data that is not 'sensitive data' in and of itself, but which could allow inferences of sensitive data, should not be covered under this criterion. For example, individual users may incidentally reveal political or religious beliefs, or other sensitive information when they voluntarily post in free form text online. In such a case, the data processing by the online service providers would not necessarily be carried out with the intent to process political or religious information about that user. To require ISPs and other online providers to police these forums or content would be impracticable. DIGITALEUROPE would encourage clarification that this criterion should **only apply where a product or service is designed to process sensitive data, or where the controller has actual knowledge that sensitive data is being collected on a large scale; it should not apply when the collection of sensitive data is incidental or merely potential.**

DIGITALEUROPE is also concerned over the view expressed in the draft guidelines that DPIAs may be needed for data that although not defined as sensitive under Article 9, should nevertheless be considered as 'processed for sensitive purposes' or may merit a DPIA due to specific use contexts. Additionally, the definition of sensitive data is not identical in all EU Member States, as Article 9 provides Member States with competence for additional specifications or limitations. The WP29 specifically points out electronic communications data, location data and financial data. Not only is this distinction difficult to apply in practice, but will rely heavily on the final language set out in the draft ePrivacy Regulation ("ePR"). **DIGITALEUROPE does not believe that the mere processing of location data or financial data should automatically be considered as sensitive data processing or 'high risk' processing, and any such the guidance goes beyond the mandate of Article 35**. Instead, we would welcome a more risk-based approach from the WP29 noting that only 'sensitive' uses of data that could lead to harm or risk to natural persons will require a DPIA. This would assist data controllers greatly on focusing on these cases.

## 5. Section III B.a.5 – Data Processed on a Large Scale

DIGITALEUROPE notes that the recommendation in the draft guidelines to extend the conduct of DPIAs to any 'large scale' data processing effectively sets aside the risk-based approach introduced by law makers in the GDPR. This criterion goes beyond the provisions set out in Article 35(3) and provides four quantitative aspects for consideration, including the number of data subjects concerned, the volume of data, the duration or permanence of processing and the geographical extent of the processing. A fifth factor focusing on the sensitivity of the data could be included here. However, these factors should not, on their own, be sufficient to constitute a high risk processing requiring a DPIA. Any data processing operation could be 'large scale' even if there are no actual risks to data subjects from the collection of data (e.g. name and address information for a mail marketing campaign). This approach will again ensure that data controllers will focus on mass producing DPIAs as opposed to focusing on those cases where a DPIA will actually assist in safeguarding privacy.

## 6. Section III B.a.6 – Datasets that have been Matched or Combined

DIGITALEUROPE notes that this criterion goes clearly beyond the provisions of Article 53(3), and believes that its inclusion without any more detail will not assist data controllers as to the precise situations where the WP29 considers that a DPIA should be conducted. The mere fact of data matching or combination should only trigger a DPIA requirement where the process results in a category of 'high risk' data listed in Article 35(3). Moreover, DIGITALEUROPE questions whether this criteria is focused on the same data controller or different data controllers matching datasets? Are the conditions different if a user has consented to the matching for a specific and specified purpose? Further clarity on this criterion, as well as the acknowledgement that data matching or combination, on its own, is not necessarily an indication of high risk processing, would be welcomed.

## 7. Section III B.a.7 – Vulnerability

DIGITALEUROPE believes that **vulnerability should be assessed on a case-by-case basis**. It should not be 'assumed' as described in the draft guidelines, particularly in the employment context. A potential vulnerability for data subjects in an employment context will **strictly depend on the type of data processing taking place and the nature of employment**. DIGITALEUROPE fully acknowledges that certain exceptional situations will lead to an imbalance of power between the employer and the employee or candidate. Equally, while the reference to children is understood in this context, further guidance is necessary in this respect as there are many cases where children use a service that is not specifically targeted at them and it should not be for a data controller to try to assess whether a child might use a service even though they are not the target audience or in some cases are explicitly excluded by the terms of service.

## 8. Section III B.a.8 – Innovative use or applying Technological or Organisational Solutions

DIGITALEUROPE cautions against the blanket position outlined in the draft guidelines that new technology or certain Internet of Things ("IoT") applications automatically leads to a high or increased risk to the rights and freedoms of natural persons. The final version of the guidelines should clarify that the **use of new technology or IoT itself does not lead to 'high risk processing' in the absence of additional 'high risk' factors**. DIGITALEUROPE urges the WP29 to avoid such an approach, which casts an air of general suspicion over new or innovative uses of technology. Indeed, there are many examples of new services or updates to existing services that are intended to improve privacy standards.

## 9. Section III B.a.9 – Data Transfers outside of the EU

DIGITALEUROPE believes that the reference to international data transfers could benefit from further clarity. The draft guidelines reference Recital 116, which notes that an entity must take into consideration the envisaged country or countries of destination along with the possibility for further transfers. The reference to Recital 116 **incorrectly implies that this Recital specifically relates to DPIAs**, rather than international data transfers in general. While DIGITALEUROPE respects the WP29 concerns of the 'risk' related to international data transfers, particularly to those jurisdictions which have a lower level of data protection than that which is found in the EU (or which the EU has not yet reviewed any such adequacy assessment), we would like to underline that, according to the same Recital 116, the **'risk' associated with an international data transfer can be mitigated through the use of 'appropriate safeguards'.** If a data controller is relying on binding corporate rules, standard contractual clauses,

or a similar EU-approved data transfer mechanism, the risk is minimised and the data transfer across borders should not implicate the 'high risk' concern. We would also stress that, under the GDPR, data transfers which comply with the provisions of Chapter 5 do not also require a DPIA on the sole basis that a data transfer takes place. DIGITALEUROPE cautions against an interpretation that an international data transfer shall be counted toward the '2 criteria' threshold for triggering a DPIA. This is especially the case as the GDPR has already imposed specific restrictions on international data transfers and this type of double regulation of a specific use of data must be avoided. DIGITALEUROPE would welcome the final guidelines to reflect the above and omit data transfers outside of the EU from the list of criteria.

## 10. Section III B.a.9 – Documentation

DIGITALEUROPE questions the legal justification set out in the draft guidelines, when the WP29 calls on organisations to "*thoroughly document the reasons for not carrying out a DPIA*" in instances where at least two of the 'high risk' criteria set out earlier in the document are met. **The GDPR does not require documentation for why organisations have chosen *not* to proceed with a DPIA, but only requires DPIAs to be documented**. DIGITALEUROPE points out that Article 24, which states that data controllers and data processors must be '*able to demonstrate*' that any processing is in accordance with the GDPR, cannot be viewed as legal justification for '*thorough documentation*' for those organisations that choose to not carry out a DPIA. As such, we would welcome clarification in the final version of the guidelines to properly reflect the scope and requirements of the GDPR.

Moreover, meeting the requirements of record of processing activities when determining the purposes of processing (Article 30(1)(b)), should serve to demonstrate the 'due diligence' by the data controller in reaching a determination of whether a DPIA is required. Running a risk assessment should be considered a sufficient preliminary step to assess the reasons for not conducting a DPIA.

## 11. Section III B.a.9 – Re-assessing DPIAs

DIGITALEUROPE welcomes the clarification from the WP29 that DPIA requirements are not retroactive and that only services and processing functions which are set to be launched after May 2018, which are considered as 'high risk', shall be required to undergo a DPIA. However, despite this clarification, the draft guidelines note that "*as a matter of good practice, a DPIA should be continuously carried out on existing processing activities*" and explicitly calls for a re-assessment of DPIAs every 3 years. The re-assessment criteria are to apply to processing which has taken place before May 2018. **This directly contradicts the basis that DPIAs are not retroactive and would in essence require a DPIA of previously established processing operations**. DIGITALEUROPE believes there is no basis in the GDPR for such a requirement and would welcome clarification that pre-May 2018 processing operations are not subject to the 3 year re-assessment requirement. Otherwise the guidelines again risks creating a focus on the quantity of DPIAs over quality.

Each data controller should be accountable for determining the re-assessment of a DPIA, based on the circumstance (including costs) and necessity, such as when a substantial change to the processing takes place and/or the purpose of the processing is changed. The factors that will be taken into consideration by the regulator could be provided as part of the guidance (e.g. provide some clarity around the factors DPAs would consider during an inspection in determining if the data controller acted in line with the GDPR).

## 12. Section III C – Seeking the views of Data Subjects

DIGITALEUROPE would request the WP29 to provide additional guidance on where it would be considered '*not appropriate*' to seek the views of data subjects when conducting a DPIA. Clarity surrounding situations where the use of data related to an unreleased product or service where confidentiality and the protection of intellectual property are imperative would be helpful for data controllers. DIGITALEUROPE believes the final guidelines should recognise that there are many ways to seek the views of data subjects such as user studies, public seeds of software, etc., which are also likely to meet this criteria.

## 13. Section III C.d – Publishing of DPIAs

Although the draft guidelines encourage data controllers to consider publishing their DPIAs, DIGITALEUROPE welcomes the clarification that **publishing a DPIA is not a legal requirement under the GDPR**. However, as some organisations may choose to do so, DIGITALEUROPE would welcome clarification that a DPIA may contain confidential, proprietary business information or intellectual property. Therefore, **publishing a risk assessment short of a full-blown DPIA would be a good solution to retain confidentiality of processes or operations.**

It would also be useful to acknowledge that the decision not to publish a DPIA or a risk assessment short of a full-blown DPIA would not carry any consequences from the DPAs, and that prior consultation would take place with the lead supervisory authority.

# CONCLUSION

DIGITALEUROPE once again wishes to thank the WP29 for providing the European digital technology industry with the opportunity to submit comments on the draft guidelines on DPIAs and how to determine 'high risk' processing. As previously noted, it is important that data controllers receive legal certainty so that all industry sectors clearly understand when they should be expected to execute a DPIA. We trust that the WP29 will make an objective judgement of the feedback it has received from all stakeholders so that the final guidelines reflect the original intentions of the legislators and focus on the quality of DPIAs rather than the quantity.

--

For more information please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Consumer and Enterprise Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

# ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

# DIGITALEUROPE MEMBERSHIP

## Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

## National Trade Associations

**Austria:** IOÖ
**Belarus:** INFOPARK
**Belgium:** AGORIA
**Bulgaria:** BAIT
**Cyprus:** CITEA
**Denmark:** DI Digital, IT-BRANCHEN
**Estonia:** ITL
**Finland:** TIF
**France:** AFNUM, Force Numérique, Tech in France
**Germany:** BITKOM, ZVEI
**Greece:** SEPE
**Hungary:** IVSZ
**Ireland:** ICT IRELAND
**Italy:** ANITEC
**Lithuania:** INFOBALT
**Netherlands:** Nederland ICT, FIAR
**Poland:** KIGEIT, PIIT, ZIPSEE
**Portugal:** AGEFE
**Romania:** ANIS, APDETIC
**Slovakia**: ITAS
**Slovenia:** GZS
**Spain:** AMETIC
**Sweden:** Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
**Switzerland:** SWICO
**Turkey:** Digital Turkey Platform, ECID
**Ukraine:** IT UKRAINE
**United Kingdom:** techUK

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20