Position Paper

Bitkom views on Article 29 Working Party draft Guidelines on Data Protection Impact Assessment (DPIA)

24/04/2017

Bitkom represents more than 2,400 companies in the digital sector, including 1,600 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom' members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Member of the Executive Board for
Security and Trust
P +49 30 27576 -223
s.dehmel@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Thorsten Dirks

CEO
Dr. Bernhard Rohleder

Overview

1. Introduction

Bitkom welcomes the opportunity to comment on the Art. 29 Working Group's (WP29) draft opinion on Data Protection Impact Assessment (DPIA). We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice.

In our working group on data protection (Arbeitskreis Datenschutz) we gather more than 600 data protection professionals, of which most are practicing data protection officers who are currently commonly working on the interpretation and application of the GDPR.

Bitkom has dedicated considerable efforts to help companies especially SMEs in planning their data protection approaches towards GDPR compliance and implementing the main changes and new features of the GDPR. In this respect, we have published a series of practical guidelines for companies including guidelines on how to carry out a risk assessment as vaguely explained in Art. 32 GDPR and a DPIA as required by Art. 35 GDPR.

In the process of drafting these practical guidelines for companies, Bitkom has extensively discussed and assessed current approaches on risk management and DPIA processes. Furthermore, Bitkom has also worked on a white listing proposal for kinds of processing operations where a DPIA is not required. Against this background, we would like to comment on the draft guidelines WP248 of the WP29 and would welcome further exchanges.

This paper firstly summarizes in **Chapter 2** the key views of our data protection working group on the clarifications presented in the draft document and further explains these views in **Chapter 3** following the structure of the WP248.

2.General remarks on Article 29 Working Party draft guidelines

- **Data Protection Impact Assessment only in exceptional cases:** While Bitkom welcomes guidance on the application of the GDPR, we are concerned that the draft opinion significantly risks shifting the paradigm: whereas **the GDPR provides for a DPIA only in exceptional cases,** data protection authorities appear to consider it **more as necessary standard procedure.** This reading departs from or even goes beyond the outcome of the extensive legislative process and political discussions preceding the adoption of the GDPR. Furthermore, it does not appear to reflect the discussions stakeholders already had with some German data protection authorities, which consider a DPIA as rather the exception than the rule.

  WP248: "As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA [...] and processing operations which meet at least two of these criteria will require a DPIA" (p.10)

- **GDPR Methodology should be used:** The very general tick-two-boxes-approach (pp. 7-10) neither describes what exactly the "high risks for the rights and freedoms of natural persons" are, nor does it consider the more principle-based and process-oriented approach in the GDPR which determines the risk level based on the

"likelihood" and "severity" for the "rights and freedoms of natural persons". This rule of thumb may especially serve SMEs as an orientation for "high risk" processing activities.

- **Given criteria and examples do not lead to a "high risk" processing per se:** There should be more clarity in the draft guidelines that the criteria and examples given in Section III A should not automatically be considered as "high risk" processing. Otherwise, we fear that SMEs will schematically use such list as one-size-fits-all approach without actually considering the GDPR provisions that require a risk assessment based on a proper risk quantification taking into account the specific technical and organizational measures implemented by the controller. This can undermine the much more differentiated approach by the GDPR.

- **Criteria of tick-two-boxes-approach not differentiated enough**: Furthermore, Bitkom is also very concerned that the broadness of this criteria list will lead to a result, whereby e.g. global companies always have to carry out a DPIA (e.g. generalising "data transfers across borders outside the EU" as a high risk criterion which would trigger a DPIA in combination with another broad criterion such as "employee data" (criteria 7)).

- **Implemented measures taken by the controller to mitigate high risk should be taken into account before DPIA is triggered:** It should be noted that a DPIA as laid down in Art. 35 GDPR is a very long, complex and cost-intensive process which is preceded by an adequate risk management process as specified in Art. 32 GDPR whereby the level of risk is determined (e.g. low risk, risk, high risk) and appropriate measures for each data processing operations are chosen. Bitkom believes the WP29 rule-of-thumb could shift the focus inappropriately from Art. 32 GDPR towards Art. 35 GDPR.

  Example: *If '1+1 = DPIA' then almost all processing situations of internationally operating companies would trigger such process as criteria like 'evaluation', 'employee data' , ' data transfer' or 'innovative use' are easily fulfilled.*

  Rather, measures implemented by a company such as pseudonymization or encryption should be taken into account as mitigating factors at early stage when applying the rule of thumb and not only once the burdensome DPIA process has been triggered as two criteria are fulfilled.

  Example*: The broad criterion of user profiling is fulfilled. However, the company has implemented robust pseudonymization techniques for user profiles and can demonstrate that it has mitigated the "high risk" with an appropriate measure, so the likelihood and severity of the risk for data subjects has been considerably reduced. Consequently, while the high-risk criterion 'profiling' has been considered in the rule-of-thumb, it should not as such be a triggering criterion for a DPIA anymore.*

- **More guidance on when a DPIA is not required:** The guidelines only focus on "when a DPIA is required". They say hardly anything about **when a DPIA is not required** which again fosters the "DPIA as a rule" instead of "DPIA as an exception". We encourage data protection authorities to not only look into blacklisting but also whitelisting certain data processing operations which do not need a DPIA.

- **Welcome open approach which DPIA procedure is chosen:** *WP248: "The GDPR provides data controllers with flexibility to determine the precise structure and form of a DPIA" (P.15).* We generally welcome that the WP29 leaves it open which risk management and DPIA procedures can be used (e.g. Standard Data Protection Model V.1.0, AGPD, ICO, CNIL, ISO/IEC DIS 29134). It should be very clear that such recognized DPIA procedures can be

equally applied by all companies in all EU member states and are mutually recognized by data protection authorities.

Example: *German companies should be free to choose whether they use the CNIL or ICO approach and should not be expected or even required to use the Standard Data Protection Model only because it has been developed in Germany.*

This is particularly important as many companies already have data management procedures in place and only need to develop their current data protection management systems in line with the GDPR requirements. The WP29 should uphold this flexibility which is extremely important for companies.

Furthermore, Bitkom welcomes:

- The clear statement DPIA needs to be carried out for processing operations "*initiated after the GDPR becomes applicable on 25 May 2018*".

- A clear indication in which intervals a DPIA should be reassessed "*3 years, perhaps sooner depending on the nature of the processing and the rate of change in the processing operation*".

- A clear indication which criteria are sufficient to evaluate whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR ("*Annex 2 – Criteria for an acceptable DPIA"*).

- Last but not least, we recommend using the definitions and concepts from the GDPR throughout the document to avoid misunderstandings. For instance, the concept of "privacy" should be replaced by the word "data protection" as used by the Charter and the GDPR. Otherwise, it needs to be noted that "privacy" and "data protection" are considered as synonymous in the paper [see III C. a) and III C. c "right to privacy" should be replaced by "right to data protection"].

3. Main elements considered by the WP248 Guidelines

This Chapter structures Bitkom comments in the following manner:

Section III DPIA: The Regulation explained:
A. What does a DPIA address?
B. Which processing operations are subject to a DPIA?

- **B.a.1. Evaluation or scoring**
- **B.a.3 Systematic monitoring**
- **B.a.4 Sensitive Data**
- **B.a.7 Data concerning vulnerable data subjects**
- **B.a.8 Innovative use or applying technological or organizational solutions**
- **B.a.9 Data Transfers across borders outside the EU**

C. How to carry out a DPIA?
D. When shall the supervisory authority be consulted? When are Residual Risks high?

A) What does a DPIA address?

Bitkom does not have comments on this section.

B) Which processing operations are subject to a DPIA?

a) When is a DPIA mandatory?

Methodology as specified in the GDPR should be used: Firstly, there should be properly explained and justified why the identified processing operations laid down in Section B are "*likely to result in a high risk*". For instance, it should be better explained:

- Why there is a "*severity*" for the rights and freedoms of natural persons.

- According to which criteria *"likelihood*" is determined as "significant" or "maximum" (e.g. according to Annex A of ISO/ IEC 29134).

- What the respective "*rights and freedoms of natural persons*" are (right to protection of personal data according to Art. 7 Charta) which need to be taken into account in the context of risk assessment ("likelihood" and "severity" for "the rights and freedoms of natural persons"). This can e.g. refer to the principles relating to the processing of data according to Art. 5 GDPR.

Controller and data protection officers need such criteria to carry out an "objective assessment" as required by Recital 76 GDPR.

Given criteria and examples do not lead to a "high risk" processing per se: Secondly, there should be further clarification that the criteria and examples laid down in Section III b do not lead to a "high risk" processing per se. The rule of thumb may especially serve SMEs as an orientation for "high risk processing activities". However, the general approach should be much more nuanced taking the methodology for "severity" and "likelihood" of the GDPR into account.

Example: *Not any marketing profile entails to a "high risk".*
Example: *Not any new technology leads to "high risk" processing.*
Example: *Not all employment relationships should automatically become subject to a mandatory DPIA.*

Criteria of tick-two-boxes-approach not differentiated enough: Thirdly, the criteria in section B need to be more specific. Otherwise, a DPIA will always be necessary especially for companies operating globally. Following aspects should be reconsidered:

WP248: As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA [...] and processing operations which meet at least two of these criteria will require a DPIA" (p.10)

- **B.a.1 Evaluation or scoring:** "**Evaluation"** is too broad as a trigger criterion for a DPIA. The focus should be on the (intended) use of the evaluation or scoring and whether that use will likely result in high risks to the rights and freedoms of natural persons (p.7).

- **B.a.3 Systematic monitoring:** It is unclear what the concept of "**monitoring**" includes. It should be clarified whether it is only about physical monitoring (e.g. via CCTV) or also IT based control (e.g. web usage monitoring, keyword filtering, etc.)(p. 8).

- **B.a.4 Sensitive data**
    - "Sensitive data" should not be a stand-alone trigger criterion, as the GDPR requires "processing on a large scale of special categories of data". The large scale of the processing should be added to avoid a limitless DPIA increase.

    - A whitelist for the processing of "sensitive data" in the employment context is urgently required because otherwise most employer data processing activities will require a DPIA (sickness data in personal files, sickness data in personal administration tools, union membership and church membership in payroll systems, etc.)

- **B.a.7 Data concerning vulnerable data subjects: "**Vulnerability" needs to be assessed on a case-by-case basis and should not be assumed, in particular in employment relationships or for candidates. Rather the existence of an imbalance of power between the employer and the employee or candidate depends on the type of processing and the specific processing situation. (p. 9)

- **B.a.8 Innovative use or applying technological or organizational solutions (recital 116):** New technology does not automatically lead to a high or increased risk to the rights and freedoms of natural persons. This is a

technophobic approach that casts an air of general suspicion over new or innovative uses of technology (p.9).

- **B.a.9 Data transfer across border outside the European Union**
  Data transfer across border outside the European Union should not be an automatic trigger for a DPIA.

  - Firstly, by making reference to Recital 115 the WP29 creates the impression that this approach is derived from the GDPR and reflects the legislators' view which is misleading as the Recital is not related to DPIA, but to international data transfers in general.

  - Furthermore, Bitkom does not see such approach grounded in the GDPR. Although the EU is taking the view that the level of data protection outside of the EEA is in principle lower and that there is a certain risk because of that, there is arguably a difference between a risk and "high risk" which triggers a DPIA, especially as there is only one more criterion needed to consider a case to have a comparable risk like the examples given in paragraph 3 of Art. 35 GDPR. This discriminates internationally operating companies per se and does not reflect an "objective assessment" on a case-by-case-analysis as provided for in the GDPR.

  - Finally, the "risk" related to such a transfer is already mitigated through the "appropriate safeguards" (Chapter 5 of the GDPR) that need to be put in place by a controller sharing data across EU-borders.

b) When isn't a DPIA required?

WP248 "Where a processing has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulated the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis"(p.11)

It would be helpful if data protection authorities actually listed the "legal basis in EU or Member State law" "where a DPIA has already been carried out as part of the establishment of that legal basis".

c) What about already existing processing operations?

"WP29 strongly recommends carrying out DPIAs for processing operations underway prior to May 2018. In addition, where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation"

It would be also helpful if the WP29 further specified based on which criteria the controller shall evaluate whether a review is "necessary", especially if he has no reason to believe that the risk represented by the processing operation has changed.

C) How to carry out a DPIA?

a) At what moment should a DPIA be carried out? No comments.

b) Who is obliged to carry out the DPIA? No comments.

c) What is the methodology to carry out a DPIA? No comments.

It would be helpful if the essence of "the rights and freedoms for natural persons" were specified in such a way that the controller can evaluate the risk for each data protection right (e.g. referring to the principles in Art 5 (1) GDPR).

d) Should the DPIA be published?

Bitkom welcomes the clarification that publishing a DPIA is not a legal requirement under the GDPR. Furthermore, we would like to point out that there is also the option to publish a "public summary", which avoids that confidential information or intellectual property is released. ISO 29134, for example, explains what content could be included in such summary.

D) When shall the supervisory authority be consulted?

As the failure to consult a data protection authority triggers high sanctions, there should be more practical details added to this section.

Annex 1

It would be helpful, especially for SMEs, if the difference of DPIA approaches were to be explained so companies could chose more easily which DPIA mechanism fits best (e.g. Standard Data Protection Model V.1.0, AGPD, CNIL, ICO, ISO 29134).