Position Paper

Bitkom views on EDPB Certification Guidelines under Regulation 2016/679

11/07/2018

1. Introduction

Bitkom welcomes the opportunity to comment on the European Data Protection Board´s (EDPB) **Guidelines 1/2018 on Certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 (GDPR)**.

A clear and assessable regular framework is needed regarding Certification in order to ensure legal certainty. 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 and reduce legal uncertainty which is why Bitkom is pleased to provide input to the Guidelines and is also looking forward to additional Guidelines that address the identification criteria to approve certification mechanisms as transfer tools to third countries or international organisations in accordance with Article 42(2) GDPR, as additional guidance on third country transfers would be helpful, also taking into consideration the specific distinctions for appropriate safeguards, e.g. Binding Corporate Rules / Codes of Conduct / Certification / Standard Data Protection Clauses.

Bitkom appreciates the Guidelines as they provide clarity and additional guidance to the, to some extent, unclear framework of the GDPR. As Certification will only take considerable effect on the market when it is transparent and therefore comprehensible and reliable, we welcome the mention that existing relevant technical standards or national regulatory and legal initiatives need to be considered when specific criteria for certification are developed. We appreciate that the Guidelines mention interoperability on

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Managing Director
Law and Security
P +49 30 27576 -223
s.dehmel@bitkom.org

Rebekka Weiß, LL.M.
Head of Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

www.bitkom.org

this point. Certification documentation should be comparable and therefore transparent, complete and comprehensive. We also welcome the assessment of the necessity of transparency of the certificates in the Guidelines. We would, however, recommend a more precise distinction between Certifications and Codes of Conducts to prevent confusion between the two. Also, further precision and more guidance are necessary to achieve further comparability and transparency which are necessary for credibility and the market success of Certifications.

We would like to further elaborate the relevant aspects below.

2. Interoperability

Certifications, seals and marks have a high potential as they can enable companies to achieve and demonstrate GDPR compliance and could also create interoperability between different legal frameworks, other certification mechanisms and standards in other domains. Certification can be a valuable tool for all parties involved: the controller, the DPA and the data subjects as Certification can deliver transparency and comparability between services and enable companies to achieve compliance and effective data protection. Bitkom therefore supports certification mechanisms. However, they need to be effective, transparent and incentivised through interoperability as the process of obtaining certification can be lengthy and companies will be less likely to invest time and money for certification if there are already various other certification requirements in place for their specific sector.

The more GDPR certification will fit into the existing or prospective certification systems, the more likely companies will see it as a useful tool for GDPR compliance. Where requirements overlap, certification should take existing measures into account.

The Guidelines, however, address this point only on a national level (page 16 mentions: *Certification bodies will need to consider how specific criteria take existing relevant technical standards or national regulatory and legal initiatives into account. Ideally, criteria will be interoperable with existing standards that can help a controller or processor meet their obligations under the GDPR.*). Bitkom would additionally like to recommend referring

to Codes of Conduct as well with regard to existing standards and instruments as the GDPR also recognizes Codes of Conduct as instruments to demonstrate GDPR compliance (Art. 40, Recital 77 GDPR).

3. Scope

In section 1.2., the Guidelines address the relevance of some specific obligations in the GDPR where certification can be used as an element to demonstrate compliance, notably in terms of technical and organisational measures and sufficient guarantees. However, we would welcome clarification whether certification is only available in instances where it is explicitly referenced in an Article, e.g. Arts. 24(3), 25(3), 28(5) and 32(3).

4. Certification Criteria and Transparency

Trust is of the utmost importance which is why confusion about certification criteria and scope should be avoided. Identical findings should therefore lead to the same attestations. Furthermore, the flexibility for the creation of certifications, seals and marks could lead to fragmentation and the market being flooded by various certifications with mainly identical scopes. Harmonized certification criteria could help avoid such a situation and further trust in certifications through comparability. The approval of certification criteria is therefore an important task and the EDPB should envisage approval as soon as possible, as clarity on the "verifiability, significance, and suitability of certification criteria" (page 10) is important to facilitate EU-wide harmonization and interoperability. We also welcome the reference that certification criteria being need to be formulated in such a way that they are clear and comprehensible and need to allow practical application.

5. Terminology

Regarding terminology it is important that Certifications and Codes of Conduct are not confused and the criteria and all guidance are clearly separated. Bitkom would therefore welcome clarifications with regard to the Guidelines´ section 2.1. on *"Supervisory Authority as certification body"*, as the paragraph includes language principally linked to Codes of Conduct:

> *It should be ensured that this certification agreement requires the applicant to comply at least with the certification criteria including necessary arrangements to conduct the evaluation, monitoring, and review including access to information and/or premises, documentation and publication of reports and results, and investigation of complaints.*

This could lead to confusion between Codes of Conduct and certification, as "monitoring" is linked to Codes of Conduct in Article 41 GDPR, whereas Article 43 mentions not "monitoring" but "periodic review" for Certifications. This distinction between Condes of Conducts (Art. 40 and 41 GDPR) and Certifications (Art. 42 and 43 GDPR) takes account of the fact that Certificates are based on a final assessment of all criteria at a certain, distinct time whereas Codes of Conduct are linked to the constant monitoring. We therefore recommend amending the paragraph accordingly to prevent mixing terminology.

6. Comparability of Criteria and their Application

Comparability of Certifications is key for the success of Certifications and trust in the market. As the purpose of Certification can only be achieved if the scheme is clear, transparent and comparable, the outcome of the certification process must be clear and reproduceable as well. Hence, the certification process must be comparable, regardless of the certifier or auditor. Transparency for Certifications (and seals or marks derived from them) is of the utmost importance for the acceptance and success on the market. Keeping this necessity in mind, we would therefore like to raise the following issue with regard to requirements derived from ISO 17065:

(a) Criteria for certification programs are now established and published by the competent bodies. The German DAkkS has promised publication of criteria until September 2018.

b) On the basis of these criteria, program owners then develop certification programs that contain specifications for certification procedures, regulations to this end are contained in ISO 17067, which are reviewed and recognized by the DAkkS.

c) Certification bodies then develop their own certification procedures on the basis of a certification program and submit these to the accreditation body for accreditation.

Criteria (a) are discussed in detail in the document, but the role of program owners (b) is practically not mentioned. In section 2 of the Guidelines the different models for certifications are listed. For the first three options, the program owner is clear, but for option 4 we would like to voice concern that there are no restrictions or criteria for these programs. According to the current status, any certification body can create its own program and then submit it for review and since certification marks and seals are part of a program, there is a real danger that there will be a multitude of competing systems here – apart from the fact that despite the same, underlying criteria, certification programs can certainly differ in claim, testing depth, etc.

We would therefore like to voice our concern on this issue and ask the EDPB to clarify and propose a suitable solution on how to safeguard comparability.