Position Paper

Bitkom views on EDPB Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

02/04/2019

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Introduction

On 12 February 2019, the European Data Protection Board (EDPB) published their Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under the GDPR and opened the corresponding public consultation.

In general, the Guidelines and the described concepts are highly welcomed. Codes of conduct, like certification, are an important part in the framework of the GDPR and one element to facilitate and demonstrate compliance with the new legislation. In our view, EU-wide codes should be included and promoted more prominently and the conditions for the approval of such Codes of Conduct should be streamlined to achieve more scale and more consistent protection across Europe. Furthermore, we need flexible and harmonised rules for monitoring bodies. Some adjustments should therefore be introduced to the Guidelines. We are therefore grateful for the opportunity to provide some detailed comments on the Guidelines 1/2019.

2. Definitions

2.1 Accreditation

In Chapter 2, the Guidelines provide that *'Accreditation' refers to the ascertainment that the proposed monitoring body meets the requirements set out in Article 41 of the GDPR to carry out the monitoring of compliance with a code of conduct. This check is undertaken by the supervisory authority where the code is submitted for approval (Article 41(1)). The accreditation of a monitoring*

body applies only for a specific code.

This definition leaves open some questions, especially with regard to transnational Codes of Conduct. If, like proposed by the Guidelines, it is made mandatory to choose the same supervisory authority for accreditation where the code is submitted for approval, it is unclear what consequences it might have if the code is assessed by different monitoring bodies in more than one member state.

2.2. Amendments to Codes

The Guidelines provide that all requirements set out in Chapter 5 (Admissibility of a Draft Code) also apply to amended or extended codes (Footnote 27). As it is required to submit amendments to already approved Codes for admissibility, further guidance is needed on what ´amended´ means. Amendments could include substantive changes or any literal change (such as a slight change in wording or grammar correction). We therefore suggest including more guidance and examples in this regard.

3. Codes of Conduct in different but broader sectors

The GDPR provides in Article 40 para 1 that codes should contribute to the GDPR's proper application 'taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.' And while the GDPR refers to specific sectors in this provision, we suggest softening of the corresponding parts in the Guidelines. The Guidelines should specifically include the possibility that Codes of Conduct can be applicable to more than a single industry sector as the GDPR itself does not provide an absolute requirement that Codes can only apply to a specific one. Especially with regard to certain data processing operations that are similar in different sectors and companies it might be appropriate to adopt largely similar solutions to achieve compliance.

The Guidelines also strictly distinguish between 'national' and 'transnational' Codes of Conduct and include requirements for transnational codes that would lead to additional layers to get a Code approved compared to the GDPR text. The GDPR itself provides for a clear and lean procedure for Codes that include processing operations in more than one EU Member State. Codes that are national in nature have to be assessed by a single

national Data Protection Authority (DPA) whereas the Code is referred to the European Data Protection Board for an opinion before it is submitted to the Commission, if it relates to processing operations on more than one Member State. The Commission is then empowered to decide for the general validity within the Union. The Guidelines, however, require the national DPA to identify and notify other concerned DPAs and include them in a joint review before the code is submitted to the EDPB. The Guidelines should therefore be amended to focus on the competence of the DPAs to determine whether a submitted Code of Conduct relates to processing activities in more than one Member State to determine whether it has to be referred to the EDPB and the Commission (Article 40 para 7 and 9 GDPR).

4. Codes of Conduct and their merit for transferring data to third countries

The upcoming Brexit will mean a major shift for many companies and their data processing operations. From the moment of the exit, the GDPR will no longer be directly applicable in the UK as the country will no longer be an EU member state. The status of the UK will thus change to “third country” in all aspects of the GDPR and this will influence all transfers of personal data. The transfer of personal data between an EU-based business and a third country will then only be possible if the third country provides for an adequate level of protection or other measures are taken to ensure that the level of data protection is not undermined. Before this background, Bitkom suggests to include more detailed provisions for Codes of Conducts in the Guidelines for transfers to third countries. We welcome that separate Guidelines were announced in this regard but seeing the merit of Codes of Conducts in assessing compliance we suggest including a specific reference in the current Guidelines as well. For clarification, it would be helpful if the Guidelines would specifically refer to the GDPR provision and include that, to the extent that the commitments requires by Article 46 para 2 lit e GDPR are references in a Code of Conduct, adherence to such a Code can serve as an appropriate safeguard for transferring data to a third country.

5. National Legislation

The Guidelines state that Codes must include specific provisions with respect to compliance with national legislation. This seems to cover not only data protection-specific obligations but also other 'relevant legal obligations under national law.' Bitkom suggests clarification what applicable national legislation means. If thereby the guidelines refer to national data protection law the following should be considered: Through GDPR the application of data protection law shall be harmonized to allow for a regulated flow of personal data inside the European Union. If applicable national legislation doesn't mean national data protection law, it would be important to clarify that as well.

6. Language Requirements

The recognition of the need of an English version for transnational codes is highly appreciated and very welcomed. Originating from the point that therefore transnational codes will always exist in minimum two languages, it is crucial to determine in a standardized way which language shall be the binding one and therefore prevails in case of conflicts. A possible and also practicable solution would be that the binding language should be the English version of the text as this would also be the language used and endorsed by the EDPB.

7. Consultation

The requirement set out in Chapter 5.8 assumes, that a (optional) consultation according to Recital 99 of the GDPR shall be completed ahead of addressing the application for a code of conduct to the CompSA. With regard to the procedure of application, it appears more productive to carry out possible consultations with other stakeholders as the members of the code owner, after having received a statement of the CompSA to the draft code applicate for and having elaborated a licensable draft code.

8. Approval

Bitkom would welcome clarification of the term ´reasonable time frame´ or the introduction of precise deadlines for the approval.

9. Engagement

In paragraph 58 the Guidelines provide that the assessment process should not serve as an opportunity to further consult on the provisions of the submitted code with the CompSA. Regarding the obligation of the DPAs to encourage the drawing up of codes of conduct pursuant to Article 40 para 1 GDPR, it is, however necessary to clarify the timeframe. As Article 57 para 1 lit. m GDPR makes clear, Code Owners have the possibility to consult before submitting their draft code ("(...) each supervisory authority shall(...) encourage the drawing up of codes of conduct pursuant to Article 40 para 1 GDPR and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40 para 5"). Therefore it would be considered very helpful to elaborate when and how this opportunity could take place.

The Guidelines further elaborate that it is important that the Code Owners are prepared and organised to address queries in an efficient and able manner. To guarantee that this requirement can be met fully, it would help to clarify what these queries could include, e.g. clarifications, responses to questions etc.

10. Monitoring Bodies

Bitkom welcomes that the Guidelines explicitly refer to Codes being monitored by either external or internal monitoring bodies and provides for a flexible approach in this regard. As relevant procedures and structures must also be provided to ensure their independence and expertise, the requirements provide for flexibility and appropriate safeguards. We suggest, however, moving Footnote 11 to the main body of the document to visibly include the possibility of a monitoring body to be accredited for more than one code.

In our view, it is also important to mention that a code cannot be approved if it doesn't identify a monitoring body. As the accreditation procedures might differ and given the

delays that might cause we suggest to include more detailed provisions on accreditation to set out consistent and harmonised criteria. Furthermore, there is no legal background discernible to make the Supervisory Authority of the Code and the Monitoring Body mandatorily the same, as Article 41 para 1 GDPR does not refer to Article 40 para 5 GDPR concerning the competence for accreditation. The GDPR therefore allowing for the Supervisory Authority regarding the accreditation of the Monitoring Body to be a different one, then the one competent for the approval of the code of conduct.

Regarding the revocation of a Monitoring Body we welcome that paragraph 86 stipulates the revocation as a possible but not definitive result. To avoid a fragmentation risk due to different handling in different CompSAs it would be well appreciated to concretize this margin of discretion. A possible concretization that a code shall not be suspended or withdrawn, if the code itself stipulates a certain appropriate grace period (e.g. 180 days) to find and implement a new monitoring body in cooperation with the CompSA, and if that doesn't work the approval of the code shall be withdrawn.