ADM e.V. | Französische Straße 8 | D-10117 Berlin

edpb
European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
sent to: EDPB@edpb.europa.eu

January 15, 2020

Reply to public consultation - Guidelines 4/2019

Dear Sir or Madam,

We are very grateful for the opportunity to participate in the public consultation on the "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default". Please allow us before to briefly introduce the ADM to you:

The **ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.** represents the private-sector market and social research agencies in Germany. It was established in 1955 and is the only trade association of its kind. At the time of writing, 67 research agencies are members of the ADM, together accounting for some 83 percent of turnover on the German market for market, opinion and social research (2.36 bn € in 2018). According to its statutes, the duties of the ADM include preserving and promoting the scientific nature of market and social research, ensuring the anonymity of individuals participating in scientific research studies, and developing codes of professional ethics and standards of research methodology.

A. Scope of the "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"

The "Guidelines 4/2019" on Article 25 Data Protection by Design and by Default" should primarily be understood as an exposition and interpretation of the legal provisions of Article 25 GDPR, as well as defining the resulting requirements regarding appropriate organisational and technical measures in more concrete and precise terms, so as to effectively implement the principles for the processing of personal data codified in Article 5 GDPR, as well as protecting the data subjects' rights and freedoms as legally standardized in the various Articles in Chapter 3 GDPR.

The ADM believes that the “Guidelines 4/2019” contain a series of important notes, which are relevant to the practices across different industries, with regard to how the processing of personal data can be implemented in conformity with the law in the specific industries. All the appropriate technical and organisational measures will, undoubtedly, each on its own contribute to the protection of personal data and the security of processing it. However, the ADM requests beyond that to examine whether, and if so how, the notes on the individual measures can be supplemented by specific notes on the way in which the effects of these various technical and organisational measures need to be combined when complex processing operations are performed on personal data, with a view to further increasing the practical relevance of the individual notes.

The suitability and appropriateness of individual concrete technical and organisational measures for protecting and safeguarding personal data varies depending on the industry-specific complex processing operations performed on personal data to which they are applied. Pseudonymisation and encryption, for example, are efficient measures for protecting and safeguarding personal data in a range of processing operations. In other processing operations, on the other hand, they are incompatible with the purposes of the processing. What all the individual technical and organisational measures have in common, however, is that the aim of a high level of protection and security for personal data can only be achieved in complex processing operations through the combined effect of various different, individually appropriate and suitable measures. The ADM therefore recommends that this holistic point of view should be emphasised even more in the “Guidelines 4/2019”.

B. Addressees of the legal provisions of Article 25 GDPR

The addressees of the legal provisions of Article 25 GDPR, and hence of the corresponding notes in the “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, are the controllers of the personal data as legally defined in Article 4(7) GDPR. Beyond this, joint controllers according to Article 26 GDPR must also be taken into account as addressees. It should therefore be emphasised that implementing the data protection measures through technological design and by selecting privacy-friendly defaults, is an important part of the decision regarding the purposes and means of processing personal data, which is constitutive of the controller’s function.

Processors as legally defined in Article 4(8) GDPR are only the addressees of the legal provisions of Article 25 GDPR, and hence of the corresponding notes in the “Guidelines 4/2019”, to the extent that they are obliged, under Article 28(3) and Article 33(2) GDPR, to assist the controller in ensuring compliance with the legal provisions of the General Data Protection Regulation. Technology providers are not themselves addressees of the provisions. For this to be the case, the General Data Protection Regulation would first have to be amended, for example in the context and as a consequence of the regular evaluations of the General Data Protection Regulation required by Article 97 GDPR.

Nevertheless, the explicit mention of processors, and especially technology providers, in the "Guidelines 4/2019" is to be welcomed. The level of data protection and data security can be significantly improved precisely by combining the actions of the three named instances. However, it needs to be taken into account that the "Guidelines 4/2019" cannot contain any data protection obligations for technology providers – and only limited data protection obligations for processors. Such obligations must in each case be worded as a "duty owed" by the controller or the joint controllers.

For example, the notes in Section 86 of the "Guidelines 4/2019" include various obligations pertaining to technology providers. These are worthy of support from the point of view of protecting and safeguarding personal data, but they have no legal traction because, as already mentioned, technology providers as such are not the addressees of the legal provisions of the General Data Protection Regulation. These obligations should therefore be reworded in such a way that they should be read as the corresponding obligations of the controllers to demand these duties of their technology providers.

C. Approved certification mechanisms and codes of conduct

The ADM explicitly welcomes the notes in the "Guidelines 4/2019" on the relevance of approved certification mechanisms pursuant to Article 42 GDPR, as legally standardised in Article 25(3) GDPR, for fulfilling the data protection requirements through technical design and by data-protection-friendly defaults. At the same time, the ADM requests that it be examined whether compliance with approved codes of conduct according to Article 40 GDPR, as a demonstration of the fulfilment by the controller of its obligations to guarantee data protection through technical design and privacy-friendly defaults, should also be explicitly included in the notes to the "Guidelines 4/2019".

Article 25(3) GDPR only refers to approved certification mechanisms according to Article 42 GDPR as an explicit means of demonstrating compliance with the legal provisions of Article 25 GDPR with regard to data protection through technical design and data-protection-friendly defaults. In contrast to this, Article 24(3) GDPR lists both compliance with approved codes of conduct as referred to in Article 40 GDPR and approved certification mechanisms as referred to in Article 42 GDPR as elements which may be used as means by which to demonstrate compliance with the obligations of the controller.

Approved certification mechanisms in accordance with Article 42 GDPR can undoubtedly contribute significantly to data protection and data security – not least in terms of the technical and organisational design of the processing operations performed on personal data and data-protection-friendly defaults in the hardware and software used. However, the corresponding potential and the specific advantages of approved codes of conduct in accordance with Article 40 GDPR should not be underestimated either. Special mention is due here particularly to the strengthening of data protection and data security through the resulting industry-wide standardisation of industry-specific processing operations

performed on personal data and through the accompanying upgrading of existing codes of professional conduct, which often – e.g. in the case of market, opinion and social research – go beyond the legal provisions of the General Data Protection Regulation in a number of aspects. These specific advantages of approved codes of conduct are a particular reason why national trade associations for market, opinion and social research in a number of European Union member states – including the ADM in Germany – are actively drawing up codes of conduct and presenting these for approval, as are the European industry associations.

Not least for this reason, the ADM recommends checking whether, and if so, how and to what extent the "Guidelines 4/2019" can contribute through appropriate notes, that the possible data protection aspects for ensuring the security of processing of personal data listed in Article 40(2)(h) GDPR being taken into account when drawing up codes of conduct for the proper use of the GDPR.

D. Digression: Self-regulation of market, opinion and social research in Germany

Over the years, the industry associations for market, opinion and social research in Germany have developed a comprehensive system of professional self-regulation, which codifies both the principles of professional ethics and research methodology of the industry. One key component of this system is the "ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics", which is accepted by many national associations throughout the world. The industry associations for market, opinion and social research in Germany have adopted the "ICC/ESOMAR Code" prefaced by a "Declaration for the Territory of the Federal Republic of Germany". The various guidelines published by the German industry associations put the principles of professional ethics of market, opinion and social research that are codified in the Code and the "German Declaration" in a more concrete form for individual research fields or research methods. At the time of writing, the eleven current guidelines are being revised so as to adjust the details of the rules of professional conduct to the legal provisions of the GDPR.

E. Conclusions

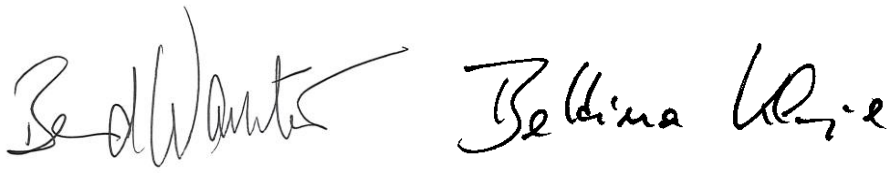
1. The “Guidelines 4/2019” on Article 25 Data Protection by Design and by Default” contain a series of notes concerning suitable technical and organisational measures for strengthening data protection and data security that are of practical relevance. This should include a stronger focus on the need to combine the effects of individually appropriate and suitable single measures in order to increase the level of protection and security of personal data.

2. The addressees of the legal provisions of Article 25 GDPR, and hence the notes of the “Guidelines 4/2019”, are the controllers or joint controllers of the personal data. In order to include processors and technology providers, it is necessary to word their specific contributions towards protecting and safeguarding of personal data as a “duty owed” by the controllers.

3. Approved certification mechanisms in accordance with Article 42 GDPR can contribute considerably to a high level of data protection and data security. This is true in particular for the aspects of an appropriate technical design and of privacy-friendly defaults. However, the potential and specific advantages of approved codes of conduct as referred to in Article 40 GDPR should not be neglected as a result of this.

Finally, we would like to once again express our gratitude for being given the opportunity to comment on the “Guidelines 4/2019”. If you have any questions or require further information, we will of course be happy to assist you.

Kind regards



Bernd Wachter
Chairman

Bettina Klumpe
Managing Director