BDO LEGAL | 2023 PRIVACY WEEK SERIES

German Data Protection Authorities' new findings on Microsoft 365 - well founded criticism or missed opportunity?

MATTHIAS NIEBUHR| BDO LEGAL - GERMANY

DSK "Findings" on Microsoft 365

On 24 November 2022, the Conference of German Data Protection supervisory authorities (DSK) published in a press release its "Findings" on Microsoft 365.

The DPA concludes that customers using MS 365 could not prove their compliance with accountability requirements based on the contractual agreement "Data Protection Addendum for Microsoft Products and Services of 15 September 2022" ("DPA") provided by Microsoft. Public authorities must not use MS 365 because of the lack of a legal basis for Microsoft's own processing. The findings are backed up by a 58-page final report of the WG "Microsoft Online Services" of 2 November 2022.

The DSK's message that MS 365 was not GDPR compliant received a lot of media attention in Germany. The comments vary between statements such as "The supervisory authorities have serious data protection concerns about Microsoft 365 " and "Microsoft 365 - this is not what data protection supervision should be".

So, is MS 365 now actually banned in Germany?

I. Legal nature of the findings, scope of the review

While the "findings" appear to be an official decision, they are, in fact, not. There is no legal basis for a binding decision by the DSK. It is an unofficial working body for the exchange of opinions between the 17 Data Protection Supervisory Authorities in Germany. Therefore, the paper is merely a coordinated legal opinion of Germany's Supervisory Authorities. Actual enforcement would require individual actions by the Data Protection Authorities.

It is noteworthy that the DSK explicitly reviewed only the DPA itself. The products concerned were not evaluated technically/functionally at all (unlike by the Dutch Government in their DPIA in 2022) and technical documentation was not included in the review.

II. The position of the DSK: Lack of transparency, processing by Microsoft for its own purposes

The DSK claims that the accountability requirement pursuant to Article 5 (2) of the GDPR is not met; as Microsoft does not fully disclose which processing activities take place in detail and whether they are performed on behalf of its customer or for its own purposes. The DPA was not precise and allowed Microsoft to carry out non-assessable, extensive processing for its own purposes.

1. Accountability

The DSK claims that the Microsoft DPA, namely its Appendix B, describes the processing activities in a "catch-all" manner, generally describing all processing operations on behalf of the client. Instead, a "specific and detailed" description of processing activities is necessary. Only by giving specific information, the customers will be able to fulfil their transparency obligations under data protection law.

Subsequently, the DSK provides various suggestions on how this can be done, for example on the basis of Appendix II of the EU standard contractual clauses or a checklist of some of the German Data Protection Authorities. The DSK also calls for a process that makes the details and the processing visible, resulting in them being part of the formal contract.

However, the DSK's statements in the report raise the question of whether they are making a (non-binding) recommendation or whether they view it, in fact, as a (real) legal requirement. In the latter case, MS 365 customers could be subject to penalties under Art. 83 (5) lit a. DSGVO, thus, the highest fine level GDPR foresees for failure to comply.

Microsoft has responded to DSK's findings criticising the requirements as excessive. The level of detail for accountability should allow the essential elements of processing to be recognisable. GDPR, however, does not require every detail of the technical implementation to be described. The DSK's requirements were impractical and hostile to technology. In addition, Microsoft refers to its extensive technical documentation provided to customers for each individual product.

Microsoft's view is understandable. As a globally active operator of a complex infrastructure, how can they ensure detailed up-to-date contractual documentation on an ongoing basis with a multitude of products and jurisdictions and thousands of users? And the main question remains whether Article 5(2) of the GDPR really requires such detailed level of information in contracts?

The two positions are difficult to reconcile and in absence of clarification by the European Data Protection Board (EDPB) and decisions by the European Court of Justice on accountability, the level of compliance required under Art. 5(2) GDPR remains unclear.

Yet, one thing is clear: an elevated and more compliant level of accountability can be implemented by MS 365 customers by setting up their own documentation of processes and conducting a Data Protection Impact Assessment for MS 365 in addition to Microsoft's documentation.

2. The discussion around Microsoft's "own" purposes

As a second point, the DSK criticises that Microsoft bases certain processing operations for their "own" purposes on legitimate interest, Art. 6 (1) 1 lit. f GDPR. As this legal basis is not available to public authorities to Art. 6 (1) 2 GDPR, MS 365 must not be used by government institutions.

The DSK's criticism relates to Microsoft's use of personal data under the DPA such as billing purposes, security measures, financial reporting or the payment of commissions to employees and partners claiming that the description lacks detail (again invoking the accountability requirement under Art. 5 (2) GDPR).

DSK's position is extreme as the stated processing operations are - regardless of their legal classification under GDPR – in fact typical and comprehensible, if not even compelling activities of any economically active company (namely controlling, accounting or financial reporting) or serve the protection of the users as well (security of processing). There are legitimate and in part even legal obligations of Microsoft as provider of the service to ensure security of processing.

The DSK itself concedes that the purposes were even included by Microsoft in the contract after consultation with the Dutch government to ensure accountability. However, DSK finds the Dutch consultation process to be non-transparent and contradicting the standards of review by the DSK and the European Data Protection Supervisor (EDPS). The DSK also broadly rejects the compatibility check approach by the French supervisory authority CNIL.

Unfortunately, the DSK - also due to a lack of any technical examination - did not take a closer look at the extent to which data is actually used by Microsoft. In their DPA Microsoft commits to adhere to the principle of data minimisation and, in particular, not to create profiles or use data for advertising or other purposes.

III. Consequences for companies and institutions

Unfortunately, DSK takes an extreme position towards the legal questions at hand. Instead of seeking a pan-EU cooperation (in accordance with section 7 GDPR) it criticises other Data Protection Authorities and adds more complexity in a time where security challenges are rising.

The findings of the DSK do not prohibit the use of MS 365, as it is a position paper and not a binding legal decision. Enforcement will require individual action by the German Data Protection Authorities.

Until the necessary Europe-wide legal clarification is reached, customers using MS 365 will face uncertainty and thus a dilemma.

This dilemma can be mitigated. Even if the Microsoft DPA - as the DSK believes - does not meet the accountability requirements, customers of MS 365 can achieve accountability by further documenting their processing using technical information by Microsoft and by supplementing it with their own process descriptions.

Particularly, conducting Data Protection Impact Assessment is advised when using MS 365 in Germany.

For further information:

MATTHIAS NIEBUHR
LAWYER | BDO LEGAL - GERMANY

+49 30 885722-770
matthias.niebuhr@bdolegal.de