AG DSK „Microsoft-Onlinedienste“

Summary of the assessment of the current agreement to order processing,

1. Investigation order, procedure and investigation object

On September 22, 2020, the DSK had an **evaluation of the working group administration** on the Online Service Terms (OST) on which the use of the cloud service Microsoft Office 365 (now: Microsoft 365) is based, as well as the data protection regulations for Microsoft online services (Data Processing Addendum / DPA) - as of January 2020 - regarding the fulfillment of the requirements of Article 28 Paragraph 3 of the General Data Protection Regulation (GDPR). The evaluation of the AK Verwaltungs came to the conclusion that *"on the basis of these documents, no data protection-compliant use of Microsoft Office 365 is possible" .*

At its meeting on September 22, 2020, the DSK asked a working group led by Brandenburg and the Bavarian State Office for Data Protection Supervision (BayLDA) to start talks with Microsoft *"to promptly make data protection-compliant improvements and adjustments to those identified by the Schrems II decision of the ECJ To achieve standards for third-country transfers for the application practice of public and non-public bodies1 ."*

As a result, a working group started talks with Microsoft at the end of 2020. Participants of the working group were: Brandenburg and BayLDA (both leaders), BfDI, Baden-Württemberg, Berlin, Hesse, Mecklenburg-Western Pomerania, Saxony, Saarland and Schleswig-Holstein. On behalf of Microsoft, employees of Microsoft Deutschland GmbH including a member of management and, depending on the focus, contact persons of Microsoft Corporation (USA) took part. As part of the talks, 14 video conferences lasting several hours took place.

During the discussions, it had to be taken into account that the lead data protection supervisory authority for Microsoft Ireland Operations, Ltd. the Irish supervisory authority is a party to the order processing contract and the German supervisory authorities are responsible for the supervision of the respective German customers (e.g. companies, authorities, i.e. the persons responsible within the meaning of Art. 4 No. 7

[1] See TOP 9 (“TOP 9 – Data protection assessment of order processing in Microsoft Office 365”), p. 5, available at: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf.

GDPR) are responsible. The main question for the German supervisory authorities was therefore whether the individual processing activities of the local controllers (for which they commissioned the processor Microsoft) are lawful and whether the order processing contract meets the requirements of Art. 28 DS-GVO. In addition, it had to be considered that the Microsoft 365 cloud service can be used in different functional scopes, variants and configurations.

The following assessments are based on the “Data Protection Addendum for Microsoft Products and Services” (hereinafter: *“Privacy Addendum”)* including the current version dated September 15, 2022. The assessment is based on the factual data as of the conclusion of the report on October 10, 2022 - and legal situation.

The report of the working group contains

a) an assessment limited solely to selected legal requirements of the GDPR, but not a complete data protection assessment of the Microsoft 365 cloud service, b) essentially an investigation based on the six from the AK Verwaltungs 2020
identified contractual defects and no additional tests
contains
c) no independent technical investigations by the working group and therefore none
Examination of the data flows and processing actually taking place,
d) no investigation of the implementation of the contractual processing or the
processing actually taking place,
e) no check of the individual components of the cloud service, in particular no check of individual functionalities for their data protection conformity (e.g. in the area of employee data protection and monitoring of employees by those responsible),
f) no examination of the individual processing activities,
g) no examination of the entire relevant Microsoft contract and h) no examination of the
data protection requirements from the TTDSG and the questions arising from telecommunications law and telecommunications secrecy.

As such, the report does not provide conclusive investigations and cannot rule out or anticipate other supervisory findings. This applies in particular with regard to

Investigations already carried out by individual supervisory authorities, some of which list independent deficiencies.2

The working group gave Microsoft an opportunity to comment before finalizing its report, reviewed this feedback, and incorporated it into its final assessments.

The following summary provides an overview of the main results of the talks and the improvements made or not made to the test points of the Administrative Working Group on which the task of the working group is based.

2. Key Findings

Microsoft released an updated Microsoft Products and *Services* Data Protection Addendum (DPA) in September 2022 . Above all, this new version brings changes in the area of the contractual wording of Microsoft's responsibility in the context of processing "for legitimate business purposes", can be seen as the result of the discussions and thus addresses some of the criticisms of the AK Verwaltungs. Overall, the working group was only able to achieve minor improvements in the points of criticism named by the Administrative Committee.

The central and recurring question of the series of talks was in which cases Microsoft acts as the processor and in which as the person responsible. This could not be finally clarified.

Responsible persons must be able to fulfill their **accountability according to Art. 5 Para. 2 DS GVO** at all times . When using Microsoft 365, difficulties can still be expected on the basis of the "data protection addendum", since Microsoft does not fully disclose **which processing takes place in detail.** In addition, Microsoft does not fully explain which processing takes place on behalf of the customer or which for its own purposes. **The contract documents are not precise in this respect** and ultimately do not allow for conclusively assessable, possibly even extensive processing, also for one's own purposes.

The use of personal data of users (e.g. employees or students) for the provider's own purposes **excludes the use of a processor in the public sector (especially in schools).** The legal basis of the entitled interest after Art. 6 (1) lit. f GDPR is not relevant for authorities (cf. Art. 6 (1) sentence 2 GDPR).

1. 2 See, for example, on the part of the German supervisory authorities: LfDI BW, available at: https://www.badenwuerttemberg.datenschutz.de/ms-365-schulen-anleitung-weiteres-vorgehen/#summary ; Berlin Commissioner for Data Protection and Freedom of Information, Notes for those responsible in Berlin on providers of video conference services, version 2.0 of February 18, 2021, p. 20 ff., https://www.datenschutzberlin.de/fileadmin/user_upload/pdf/orientation aids/ 2021 - BlnBDI Notes_Berliner_Responsible_to_Providers_Videoconferencing-Services.pdf.

Due to the difficulty for those responsible in the public sector to meet their accountability, it is also difficult to justify Article 6 Paragraph 1 lit. e GDPR in conjunction with the respective special law as the legal basis.

3. Summary of the improvements made in detail

In the following, the improvements made to the points of criticism of the AK administration are summarized after being commissioned by the DSK.

3.1. Determining the type and purpose of processing, type of personal Data

During the discussions with Microsoft, the working group was not able to **achieve any significant improvements** in the drafting of the contract with regard to the definition of the types and purposes of processing and the types of personal data processed. Improvements are still required, which should not only describe the subject of the order processing comprehensively, but also specifically and in as much detail as possible.

This could be achieved, for example, by a customer-specific specification based on the model of Annex II of the standard contractual clauses of the Commission in accordance with Art. 28 (7) GDPR. It would also be possible to provide for references to a sufficiently detailed list of processing activities (VVT) of the controller to be formally included in the contract.

3.2. Microsoft's own responsibility for processing "for legitimate business purposes" (now: "business activities")

On the subject of Microsoft's own responsibility within the framework of processing "for legitimate business purposes", the working group was able to achieve changes to the contractual structure. Regardless of different assessments of the data protection-compliant design of processing of contractual data for the processor's own purposes by the European supervisory authorities, these contractual changes do not bring about **any substantial improvements from the point of view of the working group:** The "data protection addendum" of September 2022 contains a conceptually changed section as a result of the discussions with the working group about data processing that is intended to serve Microsoft's business activities, which shows the first approaches to delimitation and specification. However, according to Microsoft, it has not made **any adjustments to the actual processing .**

From the point of view of the working group, a more detailed examination of the contractual restructuring shows that Microsoft is continuing the basic approaches of the previous regulation model, of allowing itself to be granted **insufficiently limited rights** for certain processing of the processed personal data. It remains **unclear** which personal data is processed within the scope of what Microsoft calls "legitimate" business purposes or now "business activities".

It is also unclear on which legal basis the transfer of the personal data processed in the order to Microsoft's responsibility for the subsequent processing for Microsoft's purposes, including the associated comprehensive obligation to provide evidence, takes place. The same applies to data such as **telemetry and diagnostic data,** which, to the knowledge of the working group, Microsoft collects on a large scale and basically for self-interested purposes.

There are particular difficulties for public bodies, since they cannot fall back on Article 6(1)(1)(f) GDPR.

3.3. Obeying Instructions, Disclosure of Processed Data, Compliance with Legal Obligations, CLOUD Act, FISA 702

The current data protection addendum of September 2022 contains **changes to the previous provisions that** regulate the disclosure of data provided by Microsoft as a processor for its own business purposes “to comply with legal obligations”. Although the amendments contain new wording, the powers remain similarly extensive.

The regulation restricts the customer's right to issue instructions with regard to the disclosure of the data processed in the order. The Privacy Addendum permits disclosures where required by law or as described in the "Privacy Addendum". Such disclosures are not limited to the instructions of the person responsible, so that they are only permissible against the background of Article 28 (3) subparagraph 1 sentence 2 letter a) GDPR if they relate to obligations under Union or member state law, the Microsoft subject to limit. This is not the case. As a result , **Microsoft's obligation to issue instructions does not meet the minimum legal requirements in** accordance with Article 28 (3) subparagraph 1 sentence 2 letter a GDPR.

The investigations of the working group show that Microsoft also contractually reserves the right to make far-reaching disclosures which, if **implemented, would not meet the requirements set out in Art. 48 GDPR .**

3.4. Implementation of technical and organizational measures according to Art. 32 GDPR

The version of the "data protection addendum" valid from September 15, 2022 contains **additions to the technical and organizational measures compared to the version checked by the AK administration.** Guarantee and data security measures exist for expressly restricted certain categories of data (namely customer data in "Core Online Services" and now also "Professional Services data"). In addition, Microsoft has stated that after registration it offers interested parties access to the website servicetrust.microsoft.com ("Servicetrust Website"), where information about the technical and organizational measures implemented can be viewed.

Legal uncertainties remain, since the guarantees on "security measures" formally only record a subset of the contractual personal data, namely "customer data in "core online services" and "professional service data".

3.5. Deletion and return of personal data

Microsoft explained the individual deletion processes to the working group. With the exception of the special case of processing contract data for “cyber defence” purposes, the explanations show that processing for Microsoft business purposes should not extend the deletion periods for personal data either. In addition, in the course of the redesign of the "data protection addendum", there have also been changes in relation to deletion, which, however, also entail ambiguities and contradictions.

According to the assessment of the working group, the design of the return and deletion obligation **does not always meet the legal requirements** of Article 28 (3) subparagraph 1 sentence 2 letter g GDPR. Due to the ambiguity of the regulations, those responsible cannot meet their accountability pursuant to Art. 5 Para. 2 in conjunction with Art. 5 Para. 1 Letter a DSGVO.

3.6. Information about sub-processors

The working group has repeatedly, sometimes controversially, discussed with Microsoft the design of the controller's control rights in the event of changes in the sub-processing relationships.
Despite initial reservations, Microsoft was persuaded to change the procedure, which had previously been designed as the controller's liability, to make organizational and contractual adjustments. This led to a **redesign of the notification** procedure introduced at the end of March , which led to the deletion of the previous “Get Debt” procedure in the current “Data Protection Addendum” from September 2022.

The working group understands Art. 28 Para. 2 GDPR to the effect that the information of the person responsible "about any intended change in relation to the involvement or replacement of other processors" must contain the specifically intended change and not just the general indication that changes are planned .

The sample notification e-mail provided by Microsoft only contains information about planned changes, but not the specific planned changes. The list of subcontracting relationships presented to the working group also essentially differentiates according to which service or which functionality subcontractors are used for and names their headquarters and the data categories accessible to them. In comparison, the standard contractual clauses provided by the EU Commission provide much more detailed information about the name, address and contact person of the sub-processor as well as a description of the respective processing, which should allow a clear delimitation of the responsibilities of several sub-processors used.

3.7. Data transfers to third countries

The September 2022 “Privacy Addendum” provides that **Customer authorizes Microsoft to “(…) (…) transfer Personal Data to the United States of America or any other country in which Microsoft or its sub-processors operate.”** The standard contractual clauses of the EU Commission of 2021 implemented by Microsoft apply to all transmissions of data, in particular personal data.

The discussions between the working group and Microsoft confirmed, in accordance with the contractual provisions, that personal data is transmitted to the USA when Microsoft 365 is used. **It is not possible to use Microsoft 365 without transferring personal data to the USA.** From December 2022, Microsoft plans to offer all customers in the EU area the option of storing and processing customer data, support data and other personal data of customers in the EU area (“EU Data Boundary ").

For the USA, the ECJ found in “Schrems II” that FISA 702 and EO 12333 provide disproportionate access rights for US secret services and that there is no judicial legal protection for EU citizens. In order to compensate for the fundamental rights inadequacies of FISA 702 measured against the EU standard identified by the ECJ, it would be necessary to take measures that prevent the US authorities – and thus Microsoft – from accessing personal data or make it ineffective. Many of the services included in Microsoft 365 require Microsoft to access the unencrypted, non-pseudonymized data. The obvious possibility of **encrypting the processed data is regularly not possible,** for example if the data has to be displayed in the browser. Microsoft thus has the opportunity to read data in plain text on a regular basis and ultimately for the fulfillment of contractual performance obligations. It is therefore a classic form of use case 6 of Appendix 2 of Recommendations 01/2020 of the European Data Protection Board. **For this use case, the supervisory authorities have so far not been able to identify additional protective measures that could lead to the legality of the data export.**

The measures currently provided by Microsoft in the "Location of the data at rest" section for storing the data (data at rest) do not preclude transmission, nor do they constitute sufficient protective measures. For further processing (apart from storage), the "Data Transfer and Location" section does not contain any statements on data localization. Even the measures promised by Microsoft in the "Addendum to additional protective measures" are not suitable for compensating for the fundamental legal inadequacies of US law measured against the standard of EU law.

In addition, Microsoft also contractually reserves the right to make far-reaching disclosures which, if implemented, would not meet the requirements set out in Art. 48 GDPR.

There is already a lack of an assessment basis for the transfer of personal data to **third countries other than the USA .**

Against this background, the future increased relocation of data processing to the EU, which Microsoft has already announced , **appears helpful,** but its implementation must also be observed and evaluated against the background of any extraterritorial legislation.

Whether and to what extent the Executive Order "Enhancing Safeguards for United States Signals Intelligence Activities" presented by US President Biden and Attorney General Garland on October 7, 2022 and accompanying ordinances of the US Department of Justice require changes to the conditions of the US law, is not taken into account in this report due to the fact that the implementation of these regulations is still pending