BRANDI
RECHTSANWÄLTE

THE USE OF MICROSOFT 365 IN THE COMPANY

Information on data protection I June 2024

Introduction

Microsoft 365 has become an integral part of the day-to-day work of many companies and institutions. In the area of common Office applications (such as word processing and spreadsheets), Microsoft already has a dominant market share. In addition to the Office applications, the Microsoft 365 offering also includes many other services and functions that considerably simplify and improve day-to-day business and internal organization, for example by integrating the Microsoft Teams or Microsoft SharePoint collaboration programs.

However, the use of Microsoft 365 is viewed critically from a data protection perspective, particularly by the supervisory authorities. In order to minimize existing risks, however, the responsible body can take numerous protective measures.

Usage and contract model

The services are usually offered as a cloud solution in the form of subscription models. Data is therefore regularly stored in the Microsoft cloud. However, "on premise" solutions are also offered, in which the data is stored locally on the company's own systems. This form of collaboration is certainly to be welcomed from a data protection perspective, but is probably not practicable for many companies.

A license agreement must be concluded with the service provider for the use of Microsoft 365. Since the use of the service is also always associated with the processing of personal data, an agreement on data processing in accordance with Article 28 GDPR (at Microsoft "DPA" for short) must also be concluded to ensure data protection.

Criticism of Microsoft

The use of Microsoft 365 is constantly criticized by supervisory authorities. The most frequent points of criticism relate primarily to the non-transparent data processing procedures by Microsoft and data transfers to the USA.

In addition, there is also criticism that the contract design creates considerable dependencies for customers. For example, the subscription model means that it is sometimes not possible to skip updates and use older versions of the services in the case of automatic updates. In any case, this problem means that the latest developments at Microsoft must always be carefully monitored in order to be able to quickly change the cooperation with the service provider or, in the worst case, even terminate it in the event of any practices at Microsoft that violate data protection regulations.

An example of the criticism of the supervisory authorities is the decision of the Data Protection Conference in November 2022. It came to the conclusion that those responsible cannot provide proof of data protection-compliant use on the basis of the contract documents and information from Microsoft.

Some points of criticism that are usually raised with regard to the use of Microsoft 365 are presented and categorized in more detail below.

a) Transparency at Microsoft

One risk factor in its use is the requirement to fulfill accountability obligations. According to Article 5 (2) GDPR, companies and institutions must be able to provide positive proof of compliance with data protection regulations.

This is difficult to achieve when using Microsoft 365 due to the lack of transparency in Microsoft's information on data protection. The accountability obligation offers room for interpretation as to how comprehensively proof of data protection compliance must actually be provided. The data processing model in particular, which is relevant in this case, assumes that the client does not always have full control over the entire system when using service providers. Within the limits set by the client's instructions, the service provider always has a certain amount of independent freedom of action and design.

Microsoft also argues that the abstract nature of the information provided is in the interest of protecting trade secrets and the security of technical systems. It can hardly be doubted that the more concretely the technical systems and processes are described, the easier it is for potential attackers to overcome technical security measures.

b) Data processing for own purposes
Within the scope of data processing, data may only be processed in accordance with the client's instructions. However, according to its own statements, Microsoft does not process data exclusively on the instructions of the client, but also processes certain data (such as diagnostic and telemetry data) for its own purposes. This should be clearly criticized.

However, Microsoft 365 also provides options for preventing or minimizing the processing of diagnostic and telemetry data. These technical options should also be utilized by the companies and institutions that use them. In addition, companies should inform users transparently about the use of data by Microsoft.

c) Further deficiencies in the agreement of data processing
In the design of Microsoft's DPA template, it is criticized that the processed data types and categories of data subjects are not sufficiently outlined, but only named in abstract terms.

However, it should also be noted that Microsoft has only limited control over what data is actually generated. The specific scope of use is determined by the user company and not by Microsoft as a service provider.

The lack of instruction and control rights is also criticized. This is certainly a valid criticism, but limited instruction and control rights are unfortunately part of the nature of the big players. Ultimately, however, Microsoft's customers always remain the masters of their own data and the cooperation can be terminated in the worst case scenario. It can therefore be argued that the minimum requirement for the control of clients in the area of data processing is just about met.

d) Third country transfers to the USA
Another point of criticism of the cooperation with Microsoft is the data transfer to the USA and the associated access possibilities for US security authorities.

This became particularly relevant after the Schrems II ruling in the summer of 2020, in which the EU-US Privacy Shield adequacy decision that had been applicable until then was declared invalid.

In the meantime, a new adequacy decision has been issued by the EU Commission, the EU-US Data Privacy Framework, under which Microsoft is also certified. The transfer of data to the USA can therefore currently be based on the adequacy decision. However, as there has already been significant criticism of the regulations and a renewed review by the ECJ is to be expected in the future, further developments should be monitored closely.

e) Data protection impact assessment
It is often argued that a data protection impact assessment in accordance with Article 35 GDPR must always be carried out before the service is used. However, this goes too far and the correct view is that a risk assessment must instead be carried out in the specific case to determine whether there is an increased risk to the personal data of the data subjects. A data protection impact assessment should only be carried out if there is an increased risk to the data - for example in the case of extensive processing of sensitive personal data in accordance with Article 9 GDPR. In any case, however, comprehensive documentation of the use is advisable.

Recommendations for action

Despite the criticism of Microsoft, it is possible to minimize existing risks in order to achieve data protection-compliant use of the service, even if certain residual risks always remain.

As the standard agreement is constantly updated by Microsoft, it is advisable to conclude the current version of the data processing agreement with the service provider.

Companies and institutions should comprehensively document the use of the service and use technical setting options that are as privacy-friendly as possible, for example to minimize the processing of diagnostic and telemetry data. In addition, data should only be stored in encrypted form on Microsoft's systems where possible.

In addition, organizational measures should be taken, for example by giving employees binding guidelines on the use of Microsoft 365. In this context, remote work should also be technically secured through technical measures such as VPN connections and two-factor authentication.

Hendrik Verst

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Hendrik Verst
Research Associate

T +49 521 96535 - 981
F +49 521 96535 - 113
M hendrik.verst@brandi.net