

## Microsoft 365 – Datenschutzkonform?

Jeder kennt es, viele nutzen es – Microsoft und seine Office Produkte. Und inzwischen wird mehrheitlich die cloudbasierte Version von Microsoft 365 eingesetzt. Neben allen Vorteilen, die diese Anwendung bietet, sind die datenschutzrechtlichen Risiken nicht zu vernachlässigen.

Die niederländische Datenschutzbehörde AP wurde von der Regierung beauftragt, eine Einschätzung zur Verwendung von Microsoft 365 in öffentlichen Behörden abzugeben. Die Aufsichtsbehörde kam nach einer Datenschutzfolgenabschätzung zu dem Schluss, dass Microsoft in vielerlei Hinsicht gegen das Datenschutzrecht verstößt.

### Warum wurde eine Prüfung durchgeführt?

Die Aufsichtsbehörde wurde durch die Regierung beauftragt, den datenschutzkonformen Einsatz der Microsoft Cloud mit SharePoint und OneDrive zu überprüfen. Dies beinhaltete auch die Prüfung der Web-Version von Microsoft Office 365. Da bereits vor der Einführung von Windows 10 bekannt war, dass Microsoft Daten der Nutzer auch ohne deren Einwilligung verarbeitet, entschied sich die Datenschutzbehörde eine Datenschutzfolgenabschätzung (DSFA) gemäß Artikel 35 DSGVO durchzuführen.

Da die Software in verschiedenen niederländischen Behörden, u.a. Justiz, Polizei und Steuerbehörde, eingesetzt werden soll, betrifft die Verarbeitung personenbezogener Daten nahezu alle niederländischen Staatsbürger.

### Um welche Daten geht es?

In dem Bericht wird klar, dass das konkrete Ausmaß der an Microsoft übertragenen Daten nicht bekannt ist. Problematisch ist die Übertragung der Daten in die Vereinigten Staaten, welche gemäß der Auslegung der DSGVO zu einem unsicheren Drittland gezählt werden.

Die ePrivacy-Richtlinie unterscheidet drei Kategorien von Daten:

#### 1. **Inhalt der Kommunikation**

Dies sind die Dokumente und Daten selbst. Microsoft 365 übermittelt also sämtliche Inhalte von Dokumenten und Anwendungen an die Microsoft-Server in den USA.

#### 2. **Diagnosedaten**

Dies sind Informationen über die Nutzung von Microsoft und das Verhalten des Nutzers, z.B. zur Nutzung von Apps, Browser, Freihand- und Eingabedaten. Diese Daten werden in Event Logs gespeichert und an Microsoft übermittelt

#### 3. **Funktionsdaten**

Diese Daten sind notwendig um eine Verbindung zu Microsoft herzustellen. Hierzu gehören u.a. Daten zur Authentifizierung des Nutzers oder die Information zur Gültigkeit von Lizenzen.

Allerdings nimmt Microsoft eine andere Klassifizierung der Daten vor, als es die ePrivacy-Richtlinie tut.

Durch ein Analysetool hat die niederländische Behörde festgestellt, dass zwischen 23.000 und 25.000 verschiedene Ereignisse („Event Logs“) an Microsoft übermittelt, welche dann von über 20 verschiedenen Teams ausgewertet werden.

## Welche Risiken ergeben sich durch die Nutzung?

Da Microsoft oft selbst nicht weiß, welche Daten zu welchem Zweck an die eigenen Server übertragen werden, ergeben sich unter anderem folgende Datenschutzrisiken:

- **Mangelnde Transparenz**, vor allem bei browserbasierten Versionen
- **Fehlende Zweckbindung**, sowohl für historische als auch für aktuelle Daten
- **Übermittlung von Daten außerhalb des EWR**
- **Unbestimmte Aufbewahrungsdauer von Diagnosedaten**

In der DSFA wurden insgesamt acht Punkte identifiziert, die ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellen.

## Was ist zu tun, wenn Microsoft 365 eingesetzt werden soll?

Wenn Microsoft 365 im Unternehmen eingesetzt wird (oder werden soll), sind mindestens folgende Maßnahmen zu ergreifen:

- Datenschutzfolgenabschätzung zum Einsatz der Software
- Aufnahme in das aktuelle Verzeichnis
- Unternehmensinterne Vereinbarungen zur Nutzung von Microsoft 365
- Regeln zur Einrichtung und Nutzung der Microsoft Dienste
- Systemeinstellungen für Diagnosedaten bei der Nutzung von Microsoft 365

Auch wenn der Einsatz von Microsoft-Produkten weltweit üblich und bewährt ist, sollte dieser immer hinterfragt und Alternativen in Betracht gezogen werden.

Bei der Festlegung und Umsetzung der Maßnahmen unterstützen wir Sie gerne.

## Zusammenfassung

Der Bericht der niederländischen Datenschutzbehörde stellt bereits zu Beginn klar, dass eine abschließende Bewertung aufgrund des breiten Einsatzgebietes nicht vorgenommen werden kann.

Die deutschen Aufsichtsbehörden haben sich noch nicht zum Ergebnis des Gutachtens geäußert. <sup>1</sup>

Vor Einsatz von Microsoft 365 sollten Regelungen festgelegt werden, welche auch regelmäßig überprüft und den aktuellen Gegebenheiten angepasst werden sollten. Sprechen Sie mich gerne an.



Schön, dass Sie sich für unsere Dienstleistungen im Bereich des Qualitäts- und Datenschutz-Managements interessieren. Kontaktieren Sie mich und wir entwickeln gemeinsam einen Plan für Ihre Zertifizierung, Akkreditierung oder die Umsetzung der DSGVO.

Katarina Leikert

Qualitäts- und Datenschutzmanagement

☎ 07362.95892-0

✉ [k.leikert@ibs-quality.de](mailto:k.leikert@ibs-quality.de)

## QUALITÄTS- und DATENSCHUTZMANAGEMENT



IBS Quality GmbH  
An den Eckwiesen 10  
73441 Bopfingen

[www.ibs-quality.de](http://www.ibs-quality.de)