Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Einsatz cloudbasierter Office-Systeme (insbes. Microsoft Office 365): Datenschutzrechtliche Eckpunkte

Auf der Grundlage eines DSGVO-konformen Vertrages[1] darf der Verantwortliche cloudbasierte Office-Systeme wie insbesondere Microsoft Office 365 nur unter den folgenden Voraussetzungen einführen und nutzen:

Organisatorisch

- **Erfassung der Prozesse und Bewertung der Schutzbedarfe**

  Um den adäquaten Umgang mit Daten im Unternehmen festzulegen, hat der Verantwortliche die datenschutzrechtlich relevanten Prozesse zu erfassen und ihre Schutzbedarfe jeweils zu bewerten, Art. 30 DSGVO. Da es sich bei Office 365 um eine neue Technologie mit weitreichenden Konsequenzen handelt, ist grundsätzlich eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) durchzuführen. Ein Verzicht muss sorgfältig begründet werden.

  Ein Schema zur Datenklassifikation schafft hierfür nicht nur eine schlüssige Basis, sondern vereinfacht auch die anschließende Umsetzung von Schutzmaßnahmen. Ein solches Schema sollte sowohl eine Vorgabe zur grundsätzlichen Einstufung der Daten als auch zur Kennzeichnung der Dateien enthalten. In Betracht kommt dabei auch eine automatisierte Kennzeichnung mit technisch vorgegebenen Speicherorten.

- **Autorisierung und Authentifikation**

  Die für das Access und Identity Management (Autorisierung und Authentifizierung) gewählten Verfahren müssen dem Schutzbedarf und den potentiellen Gefährdungen entsprechen. Soweit ein Hersteller (wie etwa Microsoft) Autorisierung und Authentifizierung aus einer Hand bietet, hat der Verantwortliche die damit verbundenen Vorteile und Risiken sorgfältig abzuwägen.

- **Private Nutzung und dienstliche Nutzung von Privatgeräten**

  Der Verantwortliche muss außerdem die Regeln zur privaten Nutzung von Hard- und Software festlegen. Gestattet er die private Nutzung, muss er auch berücksichtigen, dass der Mitarbeiter als privater Nutzer sein Auskunftsrecht in Bezug auf Telemetriedaten geltend machen kann.

  Sofern der Verantwortliche den Zugriff auf Daten von Geräten erlaubt, die nicht in das unternehmensweite Client-Management eingebunden sind (bspw. Privatgeräte), muss er zusätzliche Maßnahmen zur Datenintegrität und Vertraulichkeit vorsehen.

---

1 siehe dazu die Stellungnahme des AKDSB zu wichtigen vertraglichen Voraussetzungen für den Einsatz von Office 365 aus dem Jahr 2017 – noch vor Inkrafttreten der DSGVO.
Im Vorfeld ist zu klären, ob und inwiefern Microsoft als Auftragsverarbeiter oder Joint Controller handelt.

Personell

- **Verbindliche Anwendungsvorgaben**

  Der Verantwortliche muss verbindliche Vorgaben zur Anwendung der eingesetzten Systeme erlassen, bspw. in Form von Dienstanweisungen sowie – insbesondere für frei Beschäftigte – vertraglichen Vereinbarungen. Entsprechende Regularien können technisch-betrieblich (bspw. Endgeräte-Richtlinie) oder organisatorisch (bspw. Verhaltensregeln zum Umgang mit Daten) sein. In Bezug auf Kollaborations-Funktionen sollte der Verantwortliche außerdem festlegen, welche Informationen hierüber ausgetauscht werden dürfen und welche nicht.

- **Aufklärung und Sensibilisierung**

  Die Anwender müssen die Schutzbedürftigkeit der Daten, mit denen sie arbeiten, ebenso kennen wie die Verhaltensvorgaben. Der Verantwortliche muss deshalb solche Regeln nicht nur vorgeben, sondern auch klar kommunizieren.

Technisch

- **Deaktivierung nicht benötigter Tools und Funktionen**

  Der Verantwortliche sollte alle nicht benötigten Tools und Funktionen deaktivieren. Da herstellerseitig (insbesondere von Microsoft) vorgesehene Sicherheitsfunktionen mit einem erheblichen Informationstransfer verbunden sein können, muss der Verantwortliche sie auf Sinnhaftigkeit und Angemessenheit prüfen. Auch Art und Umfang der Diagnosedaten zur Programmverbesserung können stark eingeschränkt werden.

- **Verschlüsselung**

  Jedenfalls im Falle der Verarbeitung der Daten in einem Cloud-Dienst muss der Verantwortliche die Daten je nach Schutzbedarf verschlüsseln. Da der Eigentümer und Treuhänder des Schlüssels auf die Daten zugreifen kann, bedarf es dann außerdem geeigneter Vorgaben zur Schlüsselverwaltung.

Dezember 2019