audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Einsatz von Microsoft 365 unter Datenschutzgesichtspunkten ermöglichen

Zusammenfassung

Microsoft 365 (vormals als Office 365 bekannt) ist eine Werkzeugpalette bestehend aus Cloudanwendungen, Office Anwendungen und diversen Lösungen für Identitäts- und Rechteverwaltung. Die zumeist online nutzbaren Anwendungen sind für mobile Arbeitsplätze und im Home-Office besonders beliebt. Dabei fördern die Anforderungen der EU Datenschutz-Grundverordnung (DS-GVO) bei vielen Entscheidern die Bedenken in Bezug auf die Umsetzungsmöglichkeiten und Risiken, welche der Einsatz von Microsoft 365 mit sich bringen kann.

In diesem Whitepaper zeigen wir Herausforderungen beim Einsatz von Microsoft 365 sowie mögliche Lösungsansätze in Bezug auf den Datenschutz und die Informationssicherheit auf.

Problemstellung

Wie bereits aus vielen Medien[1] bekannt ist, soll Microsoft zahlreiche Telemetriedaten über die Nutzung seiner Dienste sammeln, welche personenbezogen auf die Benutzer sind und damit unter den Datenschutz fallen. Dabei ist es auf Grund der komplexen Anforderungen der DS-GVO sehr fragwürdig, ob ein Einsatz von Microsoft 365 in zahlreichen Anwendungsfällen gar nicht oder nur bedingt möglich ist. Weiterhin spielt der Ort der Datenverarbeitung sowie die Zugriffsmöglichkeiten von Microsoft als Anbieter aus einem Drittstaat eine datenschutzrechtliche Rolle. Außerdem stellt der amerikanische Cloud Act ein zentrales Sicherheitsrisiko dar, weil dieser in bestimmten Fällen US Unternehmen (und auch deren europäische Tochtergesellschaften) dazu verpflichten kann, den amerikanischen Behörden einen Zugriff auf die gespeicherten Daten zu geben.

Die Aufsichtsbehörden befassen sich ebenfalls intensiv mit den Produkten von Microsoft 365 und stehen diesen eher kritisch gegenüber. Wer als Verantwortlicher nun den möglicherweise (betriebswirtschaftlich) sinnvollen Einsatz vorantreibt, begibt sich in gefährliche Fahrwasser, was die Einhaltung des Datenschutzes, aber auch der Informationssicherheit betrifft. Letztendlich führt dies ohne weitere Maßnahmen zu erheblichen Risiken für das Unternehmen und die Geschäftsführung.

Lösungsansatz für den Einsatz von Microsoft 365

1. **Datenklassifikations- und Informationsstrategie im Unternehmen festlegen:**
   - Gibt es unterschiedlich kritische Daten (z.B. mit und ohne Personenbezug)?
   - Kennen die Mitarbeiter diese Kategorien?
   - Kennen die Mitarbeiter Behandlungsweisen, die sie auf Daten anwenden sollen (insbesondere in Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität)?
2. **Werkzeuge in Microsoft 365 sowie Prozesse identifizieren:**
   - Legen Sie fest, welche Tools aus dem Microsoft 365 Portfolio Sie einsetzen möchten und identifizieren Sie die dazugehörigen Prozesse und Verarbeitungstätigkeiten.
3. **Betriebsrat frühzeitig vor geplanter Einführung einbeziehen [sofern vorhanden]:**
   - Lassen Sie dem Betriebsrat die Produktpalette von jemandem vorstellen, dessen Kenntnisse sowohl Microsoft 365 selbst als auch die Themen Datenschutz und Informationssicherheit umfassen.
   - Das steigert frühzeitig die Akzeptanz sowie Transparenz und schafft Vertrauen.

[1] Siehe auch heise online: https://www.heise.de/newsticker/meldung/Untersuchung-Microsoft-Office-sammelt-Daten-und-verstoesst-gegen-die-DSGVO-4224823.html

4. **Datenschutz- und IT-Sicherheitsbeauftragten früh einbeziehen [sofern vorhanden]:**
   - Führen Sie die nächsten Schritte gemeinsam mit beiden Parteien durch.
5. **Prozesse und Verarbeitungstätigkeiten dokumentieren:**
   - Dokumentieren Sie die zu den ausgewählten Werkzeugen gehörigen Prozesse und Verarbeitungstätigkeiten mindestens auf Basis der Angaben in Art. 30 Abs. 1 DS-GVO, um eine Grundlage für die datenschutzrechtliche Bewertung zu haben.
6. **Testumgebung und Testgruppe etablieren:**
   - Richten Sie im Unternehmen eine ausreichend große und interdisziplinäre Gruppe zum Testen ein, die nicht ausschließlich aus der IT-Abteilung besteht, um einen bestmöglichen Anwenderbezug zu bekommen.
7. **Prozesse transferieren oder transformieren:**
   - Passen Sie Ihre Prozesse so an, dass diese auf Microsoft 365 Werkzeuge abgestimmt sind.
8. **Risikoanalyse durchführen:**
   - Führen Sie eine umfassende Risikoanalyse aus Sicht des Unternehmens (Informationssicherheit) sowie der betroffenen Personen (Datenschutz) durch.
   - Bei der Verarbeitung personenbezogenen Daten ist im Regelfall eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO bezüglich aller Ihrer in Microsoft 365 zu verarbeitenden Daten durchzuführen. Dabei können folgende Fragen hilfreich sein:
     - Welche Prozesse stellen ein datenschutzrechtliches Risiko für betroffene Personen dar?
     - Welche Prozesse stellen für Ihre als kritisch eingestuften Daten und Informationen ein Risiko dar?
     - Sind ausreichende Maßnahmen etabliert, um die identifizierten Risiken zu minimieren?
9. **Berechtigungskonzept erstellen:**
   - Erstellen Sie ein umfassendes Berechtigungskonzept inkl. der On- und Offboarding Prozesse für Mitarbeiter und Geschäftspartner.
10. **Datensicherungskonzept erstellen:**
    - Erstellen Sie als Teil der Daten- und Informationspolitik ein entsprechendes Datensicherungskonzept (Backupkonzept), welches auch die Nicht-Verfügbarkeit der Dienste in Bezug auf Ihre Prozesse betrachtet.
11. **Datenschutzrechtliche Rahmenbedingungen (zusammen mit dem DSB) erfüllen:**
    - Schließen Sie die Online Service Terms und die darin enthaltenen EU-Standardvertragsklauseln ab (https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx)
    - Stellen Sie sicher, dass die Rechte der betroffenen Personen gem. Art. 12 ff. DS-GVO erfüllt werden können. Erstellen Sie dazu einzelne Durchführungsprozesse.
    - Erstellen Sie Meldeprozesse für Datenschutz und Informationssicherheitsvorfälle.
12. **Regelungen für Mitarbeiter definieren:**
    - Erarbeiten Sie Regelungen zur Nutzung von Microsoft 365 und legen Sie diese in einer Betriebsvereinbarung oder in Ihren Richtlinien fest.
13. **Mehrstufiges Rollout-Konzept erarbeiten:**
    - Erstellen Sie gemeinsam mit dem Betriebsrat, dem DSB, dem ISB sowie allen Entscheidungsträgern ein Rolloutkonzept für die Einführung von Microsoft 365.

Autor und Ansprechpartner

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

XING **Linkedin**

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Einführung von Microsoft 365 und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung des Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis® Datenschutz und Informationssicherheit | CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de