
MORGENSTERN

MORGENSTERN

Microsoft 365 aus Sicht der Praxis

Herausforderungen und Umsetzungsmöglichkeiten unter Berücksichtigung datenschutz- und arbeitsrechtlicher Aspekte

MORGENSTERN

Grundsätzliche Herausforderungen

Wieso sollte sich ein Unternehmen mit diesen Risiken befassen?

- Microsoft 365 nicht einfach im „unbearbeiteten Auslieferungszustand“ einführen!
- Mitbestimmungsrechte des Betriebsrats
  - Einsatz der Anwendungen kann bei unterbliebener Einbeziehung durch den Betriebsrat blockiert werden
- Datenschutzrechtliche Haftungsrisiken (Bußgeld, Schadensersatzansprüche Betroffener)
- Es ist Aufgabe des Verantwortlichen, sicherzustellen und zu dokumentieren, dass die datenschutzrechtlichen Anforderungen beim Einsatz von Microsoft 365 jederzeit eingehalten werden
  - Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO

Grundsätzliche Herausforderungen

Rechtssichere Einführung möglich?

- Ja, aber …
- Kritik der Behörden und Datenschützer grundsätzlich berechtigt
- Aber:
  - Pauschale Ablehnung der „Datenschutzkonformität“ von Microsoft 365 greift zu kurz
  - Unsere DS-GVO verfolgt einen risikoorientierten und technologieneutralen Ansatz
  - DS-GVO selbst gibt Instrumente vor, risikobehaftete Verarbeitungstätigkeiten „in den Griff zu bekommen“
  - Stichwort: Datenschutz-Folgenabschätzung und technische und organisatorische Maßnahmen (TOM)
  - Microsoft hat bereits zahlreiche Nachbesserungen in Reaktion auf die Kritiken vorgenommen

Grundsätzliche Herausforderungen

Rechtssichere Einführung möglich?

- Durch eine sachgerechte Auswahl des benötigten Funktionsumfangs, ggfs. die Durchführung einer Datenschutz-Folgenabschätzung sowie die Ergreifung technischer und organisatorischer Maßnahmen kann ein weitgehend rechtskonformer Einsatz gelingen
- Gleichwohl ist der Einsatz aufgrund der aktuellen Rechtsunsicherheiten nicht risikofrei

Grundsätzliche Herausforderungen

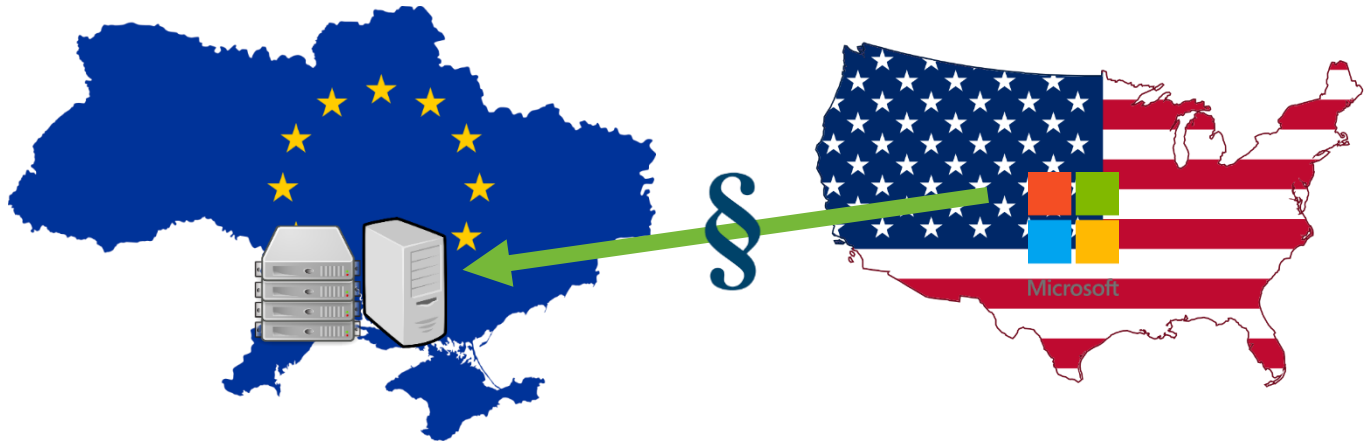
Welche Daten sollen in der Cloud „landen“?

- Vertrauliche sowie personenbezogene Daten besonderer Kategorien sollten nach Möglichkeit aus der Cloudhaltung ausgeschlossen werden
  - z.B. Daten zu Personalangelegenheiten, weil regelmäßig Gesundheitsdaten und Daten zur Religion verarbeitet werden
  - Abstufung kann anhand Datenklassifizierung erfolgen
- Welche „Cloud-Strategie“ soll verfolgt werden?
  - Vollständige Verlagerung der Daten in die Cloud oder nur teilweise?

Grundsätzliche Herausforderungen

Drittlandtransfer

- „Umzug“ in die Cloud bringt viele Vorteile mit sich, aber Erhaltung der und Gewährleistung ausreichender und risikoangemessener Datenschutzmaßnahmen kann eine Herausforderung sein
- Risiko: Drittlandübermittlung
  - USA: Schrems II und EU-US-Privacy-Shield, CLOUD-Act



MORGENSTERN

Grundsätzliche Herausforderungen

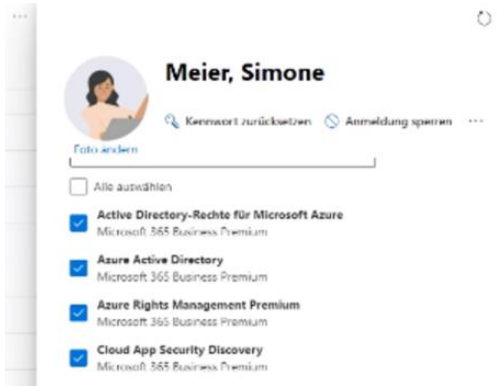
Drittstaatentransfer und „Schrems II“

- Maßnahmenempfehlungen vom EDSA (Stand: 18.06.2021), 6-Stufenmodell
  - (1) Analyse der Datentransfers in Drittländer („Know Your Transfers“)
  - (2)Identifikation der verwendeten Transferwerkzeuge
  - (3)Beurteilung der Wirksamkeit der Transferwerkzeuge
  - (4)Identifizierung angemessener ergänzender Maßnahmen
  - (5)Implementierung ergänzender Maßnahmen (z.B. Verschlüsselung, die einen Zugriff des Datenimporteurs verhindert)
  - (6)Regelmäßige Evaluierung
- Datenschutzniveau in den USA ist laut EuGH unzureichend, weswegen bei US-Dienstleistern wie Microsoft regelmäßig ergänzende Maßnahmen erforderlich sind

Grundsätzliche Herausforderungen

Deaktivierung kritischer Maßnahmen

- Komponenten können grundsätzlich für jeden einzelnen Benutzer „abgehakt“ werden



- Deaktivierung von kritischen Komponenten wie Delve und MyAnalytics auf Administratorebene für alle Benutzer (Einstellungen im SharePoint im Admin-Center unter „Delve und verwandte Funktionen deaktivieren“ oder die Nutzung jedem Benutzer selbst überlassen

- Datensammlung durch Graph wird dadurch nicht ausgeschaltet, nur die Anzeige in den Komponenten

Risikobewertung – Datenschutz-Folgenabschätzung

Vorbereitende Phase

- Stakeholder bestimmen
- Passende Lizenz bestimmen
- IT-Einsatzumgebung skizzieren und dokumentieren
- Gebuchte Microsoft-365-Dienste ermitteln
- Kritische bzw. tatsächlich nicht benötigte Dienste herausfiltern und ggfs. deaktivieren
- Geplante Verarbeitungstätigkeiten und Zwecke bestimmen und dokumentieren
- Interne Compliance- und Organisationsvorgaben berücksichtigen
- Proaktive Minimierung der „Standard-Risiken“ (Diagnose-und Telemetriedatenübermittlung)

MORGENSTERN

Risikobewertung – Datenschutz-Folgenabschätzung

- Geplante Verarbeitungstätigkeiten dokumentieren
- Rechtmäßigkeit der Datenverarbeitung
- Risiken der Datenverarbeitung herausfiltern und dokumentieren
- Berichts- und Maßnahmenphase

Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

- Ausschluss besonders vertraulicher und sensibler personenbezogener Daten aus der Cloud-Haltung
- Zugriffsrechte auf Metadaten einschränken (Stichwort Diagnose- und Telemetriedaten)
- Anwendungsbereich der Datenablage- und Bearbeitungsmöglichkeiten klar abgrenzen (SharePoint, Teams, OneDrive, Lokale Speicher)
- Deaktivierung der kritischen Anwendung bzw. nicht genutzten Anwendungen
- Rechtsänderungen für die Gültigkeit von Datentransfermechanismen (z.B. Standarddatenschutzklauseln) im Blick behalten
- Zuweisung und Festlegung der verschiedenen Administratorenrollen (so wenig globale Administratoren wie möglich); ggfs. Mehrfaktorauthentifizierung

Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

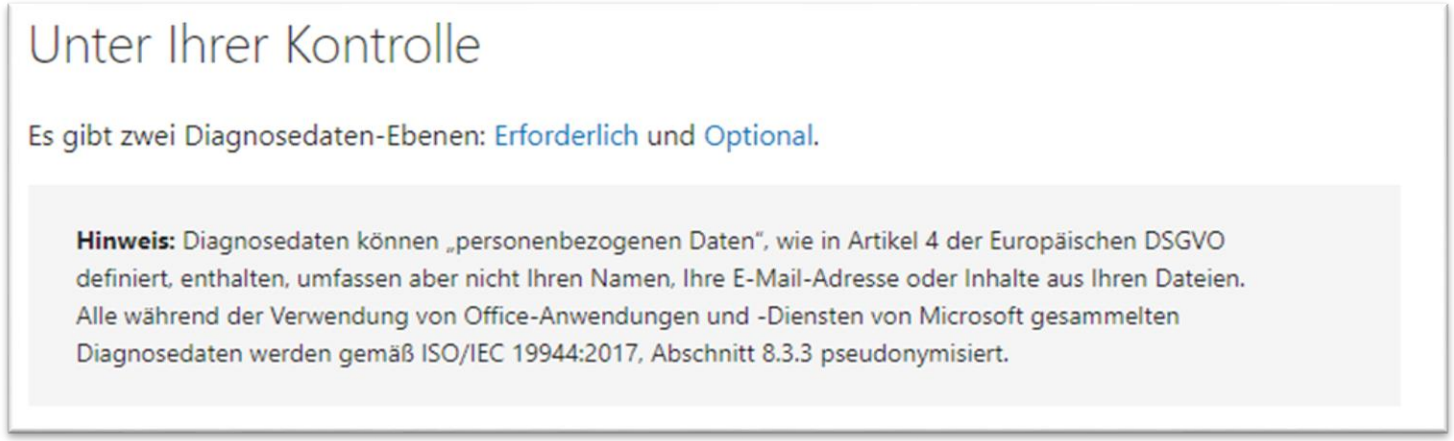
- Aktualisierung und / oder Ergänzung der internen Compliance- und Organisationsinstrumente (z.B. Richtlinien, Anweisungen)
- Nutzung des Compliance-Managers und der DS-GVO-Toolbox (soweit in gebuchter Edition enthalten)
- Verschlüsselung
  - Je nach Datenkategorie sind ggfs. zusätzliche Verschlüsselungsarten erforderlich, insbesondere wegen Drittstaatentransfer
  - „Customer key; ansonsten bleibt es bei „Microsoft managed key“

    Nicht in allen Microsoft-Plänen enthalten (Aktueller Stand: Ab Microsoft 365 E5)
- Festlegung von Sharing-Policies (Soll Sharing nur intern (z.B. innerhalb von Teams) oder auch extern möglich sein?)
- Schulung der Benutzer
  - Hilfestellung: Kostenlose Basis-Schulungsvideos von Microsoft: https://support.microsoft.com/de-de/training

Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

- Datenschutzeinstellungen
  - Diagnosedaten (https://support.microsoft.com/de-de/office/diagnosedaten-in-office-f409137d-15d3-4803-a8ae-d26fcbfc91dd)

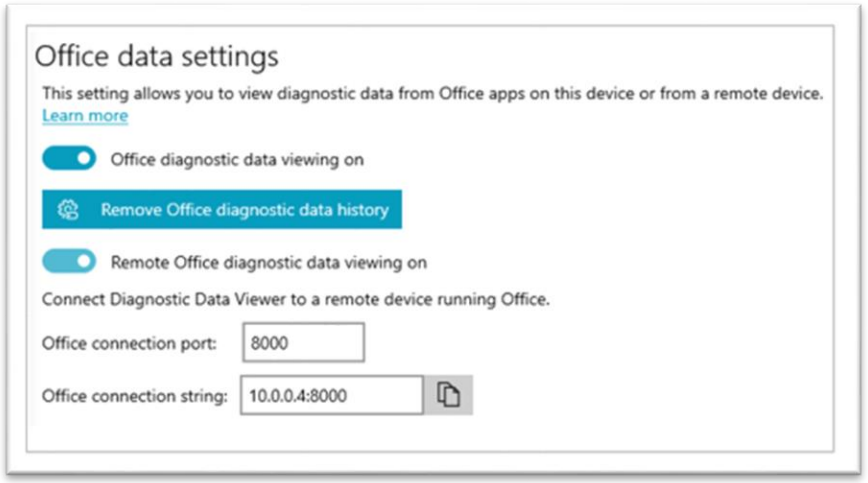


Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

- Datenschutzeinstellungen
  - Welche Daten werden an Microsoft gesendet?

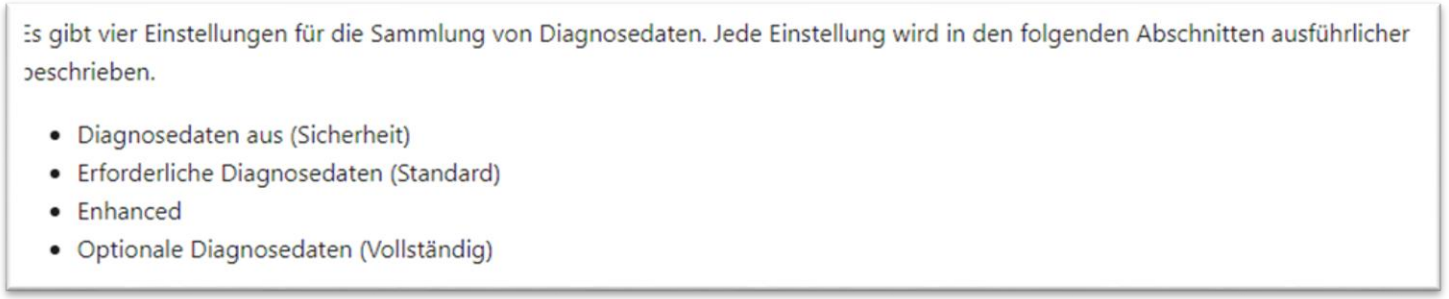
    Office Diagnosedaten-Viewer
    https://support.microsoft.com/de-de/office/verwenden-des-diagnosedaten-viewers-mit-office-cf761ce9-d805-4c60-a339-4e07f3182855



Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

- Datenschutzeinstellungen
  - Telemetrie- und Diagnosedatenübermittlung in Windows 10 auf „sicher“ einstellen
  - https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization



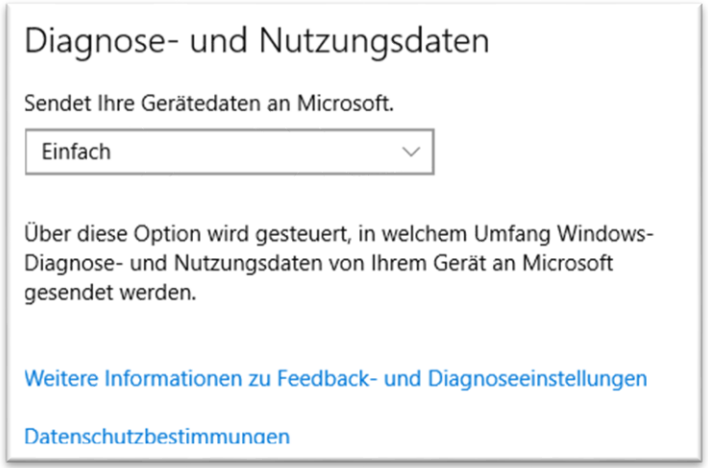
Es gibt vier Einstellungen für die Sammlung von Diagnosedaten. Jede Einstellung wird in den folgenden Abschnitten ausführlicher beschrieben.

- Diagnosedaten aus (Sicherheit)
- Erforderliche Diagnosedaten (Standard)
- Enhanced
- Optionale Diagnosedaten (Vollständig)

Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

- Datenschutzeinstellungen
  - Telemetrie- und Diagnosedatenübermittlung in Windows 10 auf „sicher“ einstellen
  - Start > Einstellungen > Datenschutz > Diagnose (oder als Administrator für jede einzelne Anwendung)
  - Bsp. Word: Optionen > Trust Center > Einstellungen für das Trust Center > Datenschutzoptionen



MORGENSTERN

Risikobewertung – Datenschutz-Folgenabschätzung

Beispiele: Technische und organisatorische Maßnahmen

- Das ist natürlich nur ein Auszug der möglichen Maßnahmen
  - Bestimmung der TOM ist ein individueller und vom Funktionsumfang abhängiger Prozess
  - Tools und Features wie das „GDPR Dashboard“ oder der „Compliance-Manager“ (mit Anzeige eines „Compliance-Scores“) können bei der Dokumentation und Auswahl hilfreich sein
  - DS-GVO Aktionsplan von Microsoft:

    https://docs.microsoft.com/de-de/compliance/regulatory/gdpr-action-plan

Weitere Schritte und Datenschutz-“Pflichtprogramm“

- Abschluss der erforderlichen datenschutzrechtlichen Verträge und Dokumentation der abgeschlossenen Versionen
- Einwilligungsmanagement bezüglich einwilligungsbedürftiger Datenverarbeitungen
- Pflichtinformationen ergänzen bzw. neu erstellen und rechtzeitig bereitstellen / einbinden
  - Die Betroffenen müssen insbesondere über die umfangreiche Analyse und Auswertung ihrer Nutzerdaten aufgeklärt werden
  - Je nachdem, für welche Zwecke diese Auswertungen genutzt werden, ist wahrscheinlich eine Einwilligung erforderlich

MORGENSTERN

Weitere Schritte und Datenschutz-“Pflichtprogramm“

- Verzeichnis von Verarbeitungstätigkeiten ergänzen
- Sensibilisierung der Mitarbeiter
- Bei Einsatz externer Dienstleister zur Einführung: Auftragsverarbeitungsvertrag?
- Verpflichtung der Administratoren auf Vertraulichkeit
- Oft sinnvoll, da über die „normale“ Administratoren-Tätigkeiten besonders umfassende Einblicke in sensible und vertrauliche Daten möglich sind (je nach Administratorenrolle)

Weitere Schritte aus arbeitsrechtlicher Sicht

Einbeziehung der Mitarbeitervertretungen

- § 80 Abs. 2 Nr. 2, Nr. 3 LPersVG RLP, § 87 Abs. 1 Nr. 6 BetrVG
- Betriebsrat darf mitbestimmen bei der Einführung, Anwendung, Änderung oder Erweiterung technischer Einrichtungen und Verfahren, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen

DEUTSCHER GEWERKSCHAFTSBUND

20.12.2017

SmartUnion

Darum ist Microsoft Office 365 ein Fall für den Betriebsrat

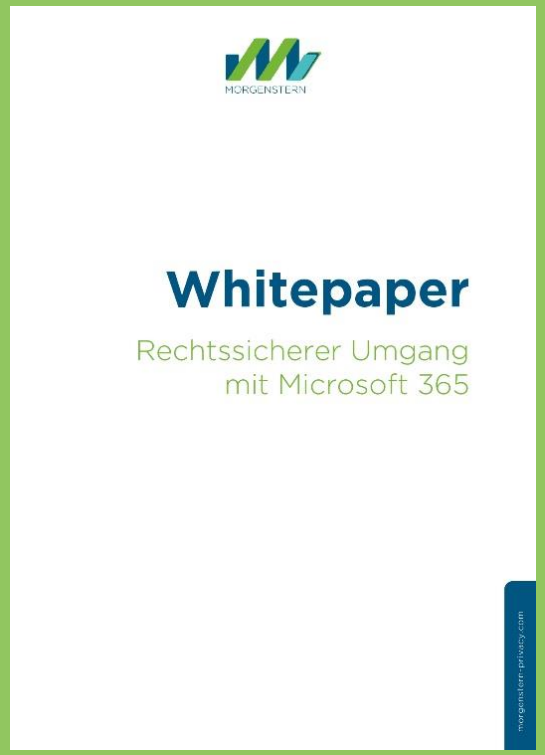
DGB-Rechtsexperte: „Einsatz von Microsoft Office 365 ist mitbestimmungspflichtig“

Mehr Effizienz durch umfassende Leistungskontrolle im Job? Mit einem neuen Add-on für die Bürosoftware Microsoft Office 365 können Arbeitgeber die Leistung ihrer MitarbeiterInnen detailliert analysieren. Aus Sicht des DGB ist der Einsatz der Software im Betrieb zwingend mitbestimmungspflichtig.

MORGENSTERN – Praxis-Tipps

MORGENSTERN
Praxis-Tipps

Rechtssicherer Umgang mit Microsoft 365



Was man alles beachten muss!

Das und vieles mehr erfährst du in unserem Whitepaper.

Hier geht´s zum Whitepaper

morgenstern-legal.com

morgenstern-privacy.com

MORGENSTERN Praxis-Tipps

MORGENSTERN Podcast – JETZT REINHÖREN!

Hier geht´s zum Podcast

MORGENSTERN

Wir sind für dich da!

MORGENSTERN

Große Himmelsgasse 1
D – 67346 Speyer
T +49 (0) 6232 – 100 119 44

speyer@morgenstern-privacy.com