
DATENSCHUTZ
AM MITTAG
11.03.2025
Datenschutz und M365
Risiken, Lösungen, Best Practices

Herzlich Willkommen!

Dr. Olaf Koglin
Rechtsanwalt,
Geschäftsführer LegalCheck
olaf@koglin.de

LEGAL CHECK
www.legalcheck.digital

Fokus dieses Vortrags

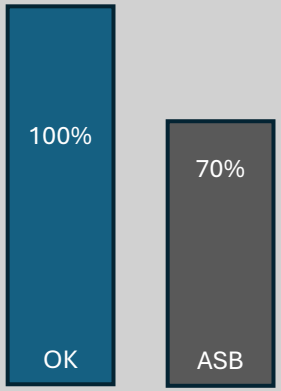
Datenschutzrecht.
Keine Daten- oder Standortpolitik.

Keine Werbung für Microsoft.
Nutzen Sie, was Sie wollen. Aber im Vortrag heute geht es halt um M365.

Kein Behörden-Bashing.
Aber teils verschiedene Meinungen

Fortsetzung folgt
Datenschutz am Mittag
25.03.2025

Übereinstimmung mit einer Position:



Olaf Koglin | Aufsichtsbehörden

- **Rechtswissenschaft: Verschiedene Meinungen sind OK**
- **Meist Einigkeit bei den ersten 9 Stufen der Gesetzesauslegung**
- **Nur bei der letzten Stufe unterschiedliche Auslegungen …**
- **und damit dann unterschiedliche Ergebnisse.**

Agenda

- Fokus dieses Vortrags
- Überblick Microsoft-Vertragswerk:
  Product Terms, DPA, EU Data Boundary
- Kritik der Aufsichtsbehörden – was davon ist (noch) berechtigt?
- Zusatzvereinbarung Niedersachsen und andere Rahmenverträge
- Lösungen und Praxis-Tipps
- Copilot
- Meine Wünsche

Das Microsoft-Vertragswerk

= https://use365.ms/PT

https://www.microsoft.com/licensing/terms/welcome/

Microsoft | Licensing Learn Purchase Manage Get Support

Please provide feedback on the new Product Terms site using the feedback button below. You may continue to access prior and cu… …oduct Terms and Online Services Terms documents here.

Product Terms

Search Terms

Select a program

Product Terms
Introduction
Summary of Changes
Universal License Terms
For Online Services
For all Software
Privacy & Security Terms
Product Offerings
Software
Online Services
Glossary
Other Legal Terms

Other Documents
Data Protection Addendum
Service Level Agreement
Microsoft Enterprise AI Services Code of Conduct

Licensing Resources
Purchasing & Renewing Software Assurance
Subscription License Suites
Licensing Briefs
Licensing Program Guides

2.

1.

Das Datenschutz-Dokument

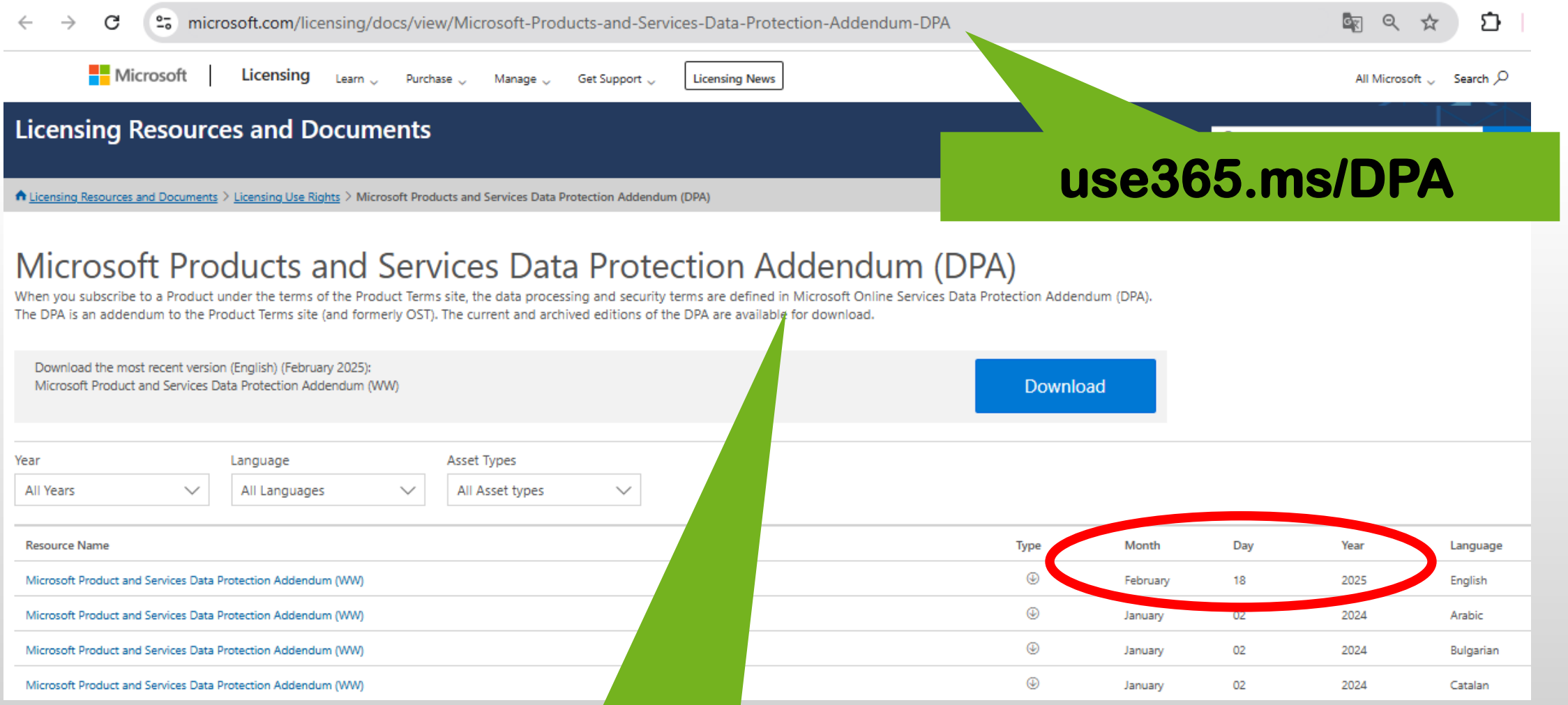
Introduction

The terms formerly contained in the "Online Services Terms" have been moved into the "Product Terms" and no longer exist as a standalone document. The unified Product Terms are incorporated by reference into agreements governing Customer's use of Microsoft Products and Professional Services. Updates that Microsoft makes from time to time to Use Rights apply to Customer as set forth in Customer's agreement.

All references to the following terms in applicable Microsoft agreements now refer to corresponding sections in the Product Terms, or to linked content within the Product Terms.

Previous Reference	Location in Product Terms
Use Rights	Located at the "Use Rights" tab within each product offering entry at Product Offerings.
Product Terms	This site.
Online Services Terms	The terms formerly contained in the Online Services Terms have been moved into the Product Terms and no longer exist as a standalone terms.
…Terms	See left navigation.
Produ…	See Product Offerings.
	…uct offering entry at:

Getting Started



„DPA“ steht für Data Protection Addendum,

nicht Data Processing Agreement (AVV).

Deutsch: „Datenschutznachtrag“

LEGAL CHECK
www.legalcheck.digital

DPA-Update nicht automatisch

Scope: „Products & Services“. Ohne 3rd Party, Preview, local

AVV

SDK („SCC“) V2021 Modul 3 Microsoft IRL (MIOL) – MS Corp.

EU Data Boundary

Zusätzlich für USA: EU-US DPF (bzw. CH / UK-Varianten)

TOMs *entspr.* ISO 27001

Für Core Online Services zusätzl.: Appendix A

Sowie (stets) Attachment 1

Microsoft

Microsoft Products and Services Data Protection Addendum

Last updated February 18, 2025

Published in English on February 18, 2025. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of February 18th, 2025.

Contents

Introduction

The parties agree that this Microsoft Products and Services Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data in connection with the Products and Services. The DPA is incorporated by reference into the Product Terms and other Microsoft agreements. The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer's volume licensing agreement or other applicable agreements in connection with the Products and Services ("Customer's agreement"), the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Professional Services Data, or Personal Data, as defined herein.

Das Microsoft-Vertragswerk

2.

https://www.microsoft.com/licensing/terms/welcome/

Microsoft | Licensing Learn Purchase Manage Get Support Licensing News All Microsoft

Please provide feedback on the new Product Terms site using the feedback button below. You may continue to access prior and current versions of the Product Terms and Online Services Terms documents here.

Product Terms

Program: None selected — Effective Date: Present Day Terms

- None selected
- Enrollment for Education Solutions (EES)
- Enterprise/Enterprise Subscription/Server and Cloud Enrollments (EA/EAS/SCE)
- Microsoft Customer Agreement
- Microsoft Online Subscription Agreement (MOSA)
- Microsoft Product and Services Agreement (MPSA)
- Open License (OL)
- Open Value / Open Value Subscription (OV/OVS)
- Open Value Subscription for Education Solutions (OVS-ES)
- Select/Select Plus (S/S+)

Search Terms

Select a program

- Product Terms
- Introduction
- Summary of Changes
- Universal License Terms
  - For Online Services
  - For all Software
- Privacy & Security Terms
- Product Offerings
  - Software
  - Online Services
- Glossary
- Other Legal Terms

Other Documents

- Data Protection Addendum
- Service Level Agreement
- Microsoft Enterprise AI Services Code of Conduct

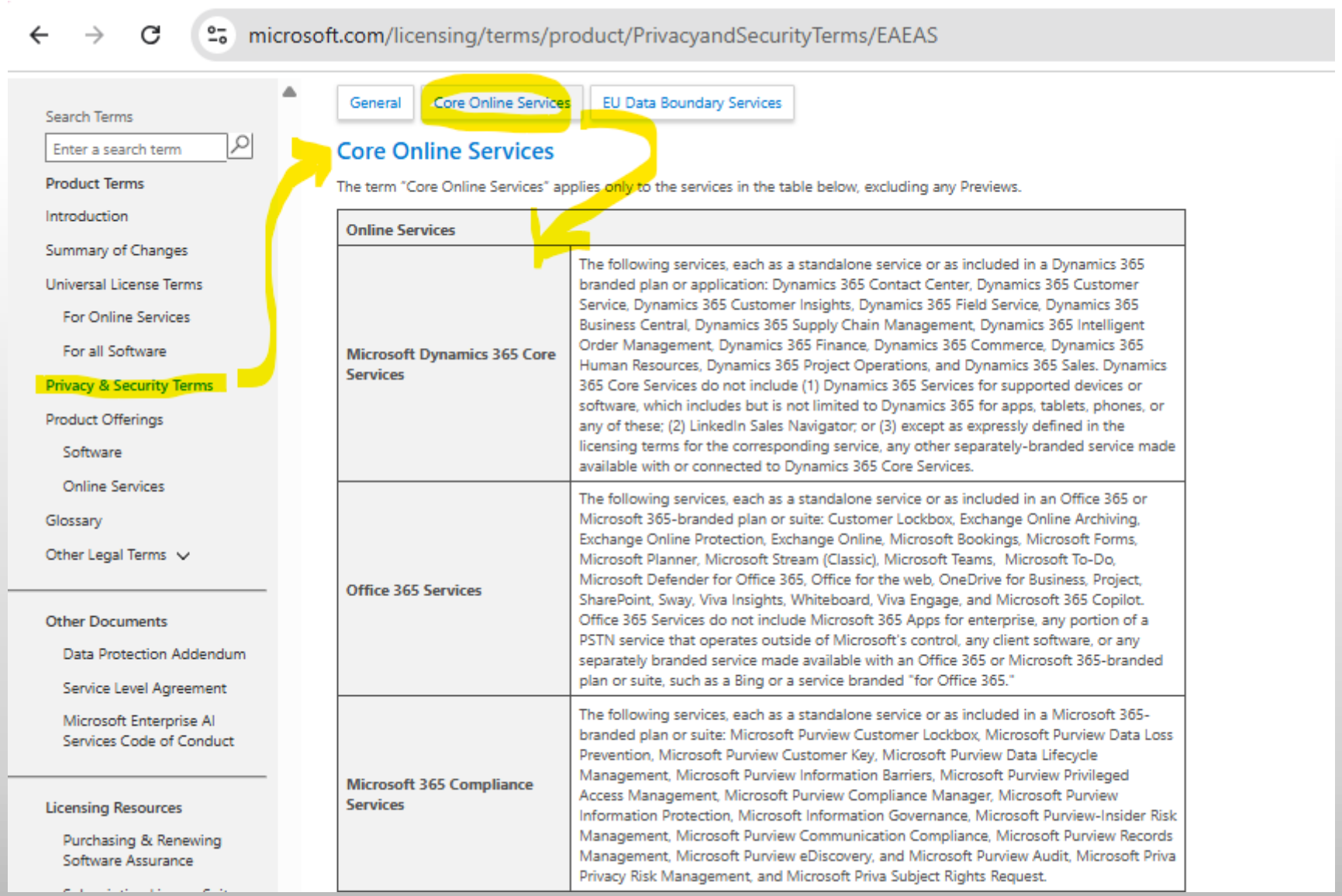
Licensing Resources

Introduction

The terms formerly contained in the "Online S
the "Product Terms" and no longer exist as a
Product Terms are incorporated by reference
use of Microsoft Products and Professional Se
from time to time to Use Rights apply to Cust
agreement.

All references to the following terms in applic
to corresponding sections in the Product Term
Product Terms.

Previous Reference	Location in Product Terms
Use Rights	Located at the "Use Rights" tab within each product offering entry at Product Offerings.
Product Terms	This site.
Online Services Terms	The terms formerly contained in the Online Services Terms have been moved into the Product Terms and no longer exist as a standalone terms.
Other Legal Terms	See left navigation.
Product-Specific License Terms	See Product Offerings.
License Model Terms	Located at the "License Model" tab within each product offering entry at:



Microsoft Products and Services Data Protection Addendum

EU Data Boundary

Last updated February 18, 2025

Published in English on February 18, 2025. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of February 18th, 2025.

Contents

Data Transfers and Location

Data Transfers

Location of Customer Data

For EU Data Boundary Online Services, Microsoft will store and process Customer Data, Personal Data, and store Professional Services Data at rest within the European Union as set forth in the Product Terms.

ft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS

General | Core Online Services | EU Data Boundary Services

EU Data Boundary Services

The term "EU Data Boundary" means the Microsoft computers, computing environment, and physical data centers located solely in the European Union (EU) and the European Free Trade Association (EFTA). The term "EU Data Boundary Services" applies only to the Online Services in the table below, excluding any Previews.

EU Data Boundary Services	
Azure	Azure services that enable deployment in a region within the EU Data Boundary and the following non-regional services: Azure Active Directory B2C, Azure Advisor, Azure Bot Service, Cloud Shell, Azure Communication Services, Azure Data Box, Azure DNS, Microsoft Entra ID, Microsoft Fabric, Azure Kubernetes Service on Azure Local, Azure Lighthouse, Azure Managed Applications, Azure Migrate, Azure Monitor, Azure Resource Manager, Azure Resource Mover, Azure Service Health, Azure Sphere, Azure Stack Edge, Azure Local, Azure Stack Hub, Azure Virtual Desktop, Azure VM Image Builder, Power BI Embedded, Traffic Manager, Translator
Dynamics 365	Dynamics 365 Business Central, Dynamics 365 Commerce, Dynamics 365 Customer Insights, Dynamics 365 Customer Service, Dynamics 365 Customer Voice, Dynamics 365 Field Service, Dynamics 365 Finance, Dynamics 365 Guides, Dynamics 365 Intelligent Order Management, Dynamics 365 Project Operations, Dynamics 365 Remote Assist, Dynamics 365 Sales, Dynamics 365 Supply Chain Management
Microsoft 365	Cloud PC, Customer Lockbox, Exchange Online, Exchange Online Archiving for Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Stream (Classic) (on SharePoint), Microsoft Teams, Microsoft To-Do, Office for the web, Online Services provided as part of Microsoft 365 Apps, OneDrive for Business, SharePoint Online, Sway, Whiteboard, Viva Engage, Microsoft 365 Copilot, Microsoft 365 Copilot Chat, Communications Compliance, eDiscovery and Audit, Insider Risk Management, Information Barriers, Microsoft Purview Data Loss Prevention, Microsoft Intune, Priva Privacy Risk Management, Priva Subject Rights Management, Microsoft Viva Answers, Microsoft Viva Connections, Microsoft Viva Engage, Microsoft Viva Glint, Microsoft Viva Goals, Microsoft Viva Insights, Microsoft Viva Learning, Microsoft Viva Pulse, Microsoft 365 Copilot for Sales, and Microsoft Viva Topics
Power Platform	Microsoft Power Apps, Microsoft Power Automate, Microsoft Power BI, Microsoft Power Pages, Microsoft Copilot Studio

Location of Customer Data, Personal Data, and Professional Services Data for EU Data Boundary Services

For EU Data Boundary Services, Microsoft will store and process **Customer Data** and **Personal Data**, and store **Professional Services Data** at rest within the EU Data Boundary as detailed below.

Customer must configure EU Data Boundary Services as follows:

Wie aktiviert man EU Data Boundary?

Agenda

- Fokus dieses Vortrags
- Überblick Microsoft-Vertragswerk:
  Product Terms, DPA, EU Data Boundary
- Kritik der Aufsichtsbehörden – was davon ist (noch) berechtigt?
- Zusatzvereinbarung Niedersachsen und andere Rahmenverträge
- Lösungen und Praxis-Tipps
- Copilot
- Meine Wünsche

Microsoft 365 und Datenschutz

Drittlandtransfer USA

Dokumentation & Rechenschaft

AVV & „Eigene Zwecke“ etc.

Technische Analyse

Alternativen & Restrisiken

Microsoft 365 und Datenschutz

Der (verfassungs-)rechtliche Rahmen

Drittlandtransfer USA

Dokumentation & Rechenschaft

AVV & „Eigene Zwecke“ etc.

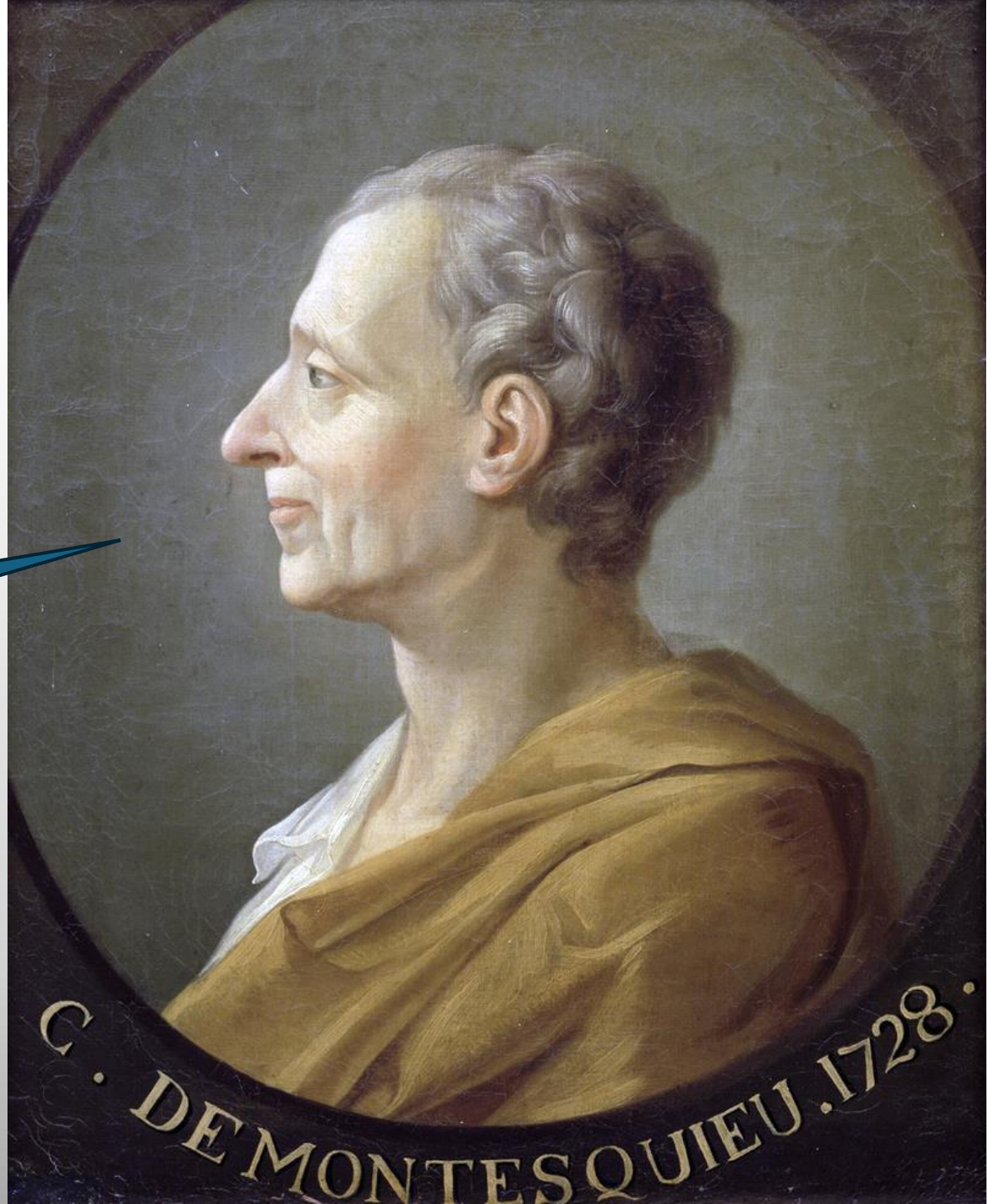
Technische Analyse

Alternativen & Restrisiken

1689

Rechtsstaat und Gewaltenteilung

1789



Der (verfassungs-)rechtliche Rahmen

- 1689 / 1789 oder: Die Gewaltenteilung; ASB als Exekutive

- Primär- und Sekundärrecht der EU:
  EU-Grundrechte-Charta und AEUV als Primärrecht,
  „Rechtsakte“ (insb. VO und RL) als Sekundärrecht.

  => Die DSGVO ist nicht die einzige Norm und kein „Super-Grundrecht“

- Zuständigkeit und Rolle der Datenschutz-Aufsichtsbehörden:
  Keine Bewertung von Produkten (wie M365), sondern Aufsicht über konkrete Verarbeitung pbD

- Spannbreite der vertretbaren Meinungen und ASB-Positionierung:
  Die Aufsicht sollte am strengeren Ende der Meinungen sein


Presets
A
B
A▸B
Routing
Settings
Auslegung: Eher viel gestattet
12.0
6.0
0.0
-6.0
-12.0
12.0
6.0
0.0
-6.0
-12.0
Auslegung: Eher strenger Datenschutz

Microsoft 365 und Datenschutz

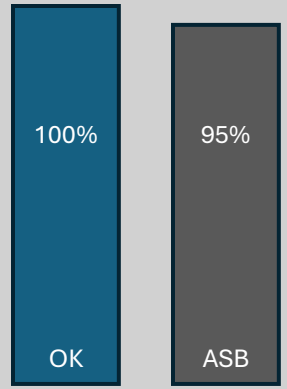
0. Der (verfassungs-)rechtliche Rahmen

- 1689 / 1789 oder: Die Gewaltenteilung; ASB als Exekutive
- Primär- und Sekundärrecht der EU:
  EU-Grundrechte-Charta und AEUV als Primärrecht,
  „Rechtsakte“ (insb. VO und RL) als Sekundärrecht.

  => Die DSGVO ist nicht die einzige Norm und kein „Super-Grundrecht“
- Zuständigkeit und Rolle der Datenschutz-Aufsichtsbehörden:
  Keine Bewertung von Produkten (wie M365), sondern Aufsicht über konkrete Verarbeitung pbD
- Spannbreite der vertretbaren Meinungen und ASB-Positionierung:
  Die Aufsicht sollte am strengeren Ende der Meinungen sein
- Errare humanum est:
  Nicht immer werden die ASB-Meinungen vom EuGH bestätigt

Rahmen

Vermutete Übereinstimmung mit dieser Auffassung:



Olaf Koglin | Aufsichtsbehörden

LEGAL CHECK
www.legalcheck.digital

LEGAL CHECK
www.legalcheck.digital

Microsoft 365 und Datenschutz

Drittlandtransfer USA

Drittlandtransfer (oder: „-übermittlung“)

- Status des EU-US Data Privacy Framework:
  - Kommissionsbeschluss (kein Vertrag)
  - In Kraft, bis Kommission revidiert oder EuGH aufhebt

- Standarddatenschutzklauseln:
  - In Kraft
  - TIA: Ist Sache zwischen SDK-Parteien, also MIOL und Microsoft USA
  - Achtung, Lücke in § 80 Abs. 2 SGB X:
    Nur Angemessenheitsbeschluss gem. Art. 45 DSGVO ausreichend,
    nicht geeignete Garantien gem. Art. 46 DSGVO wie SDK.

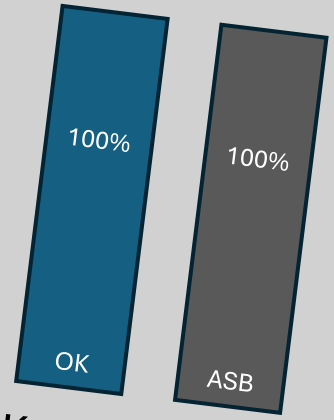
- EU Data Boundary
  - Werden überhaupt pbD in Drittland übermittelt?

DPF: Anfrage an die Aufsichtsbehörden

Frage:

4. Ist die Rechtsauffassung Ihres Hauses zum aktuellen Zeitpunkt – also u.a. vor dem Hint
der Umstände, die im Schreiben des LIBE-Ausschusses des Europäischen Parlament
Europäische Kommission vom 06.02.2025 aufgeführt wurden – dass der Kommissionsb
zum EU-US Data Privacy Framework i.S.d. § 21 Abs. 1 BDSG rechtswidrig ist?

Übereinstimmung mit dieser Auffassung:



Olaf Koglin | Aufsichtsbehörden

Antwort DSK:

einzulegen. Bei dem Angemessenheitsbeschluss handelt es sich
Solange der Angemessenheitsbeschluss in Kraft ist, kann er als
für Übermittlungen personenbezogener Daten in die USA herange

Antwort zu 1. und 2.:
Bis gegenwärtig gab es noch keinen Fall einer Antragstellung nach § 21 Abs. 1 BDSG aus dem Kreise der Datenschutzaufsichtsbehörden von Bund und Ländern in Bezug auf einen der Angemessenheitsbeschlüsse der Europäischen Kommission nach Art. 45 DSGVO.

Microsoft 365 und Datenschutz

Drittlandtransfer USA

Dokumentation & Rechenschaft

Kritikpunkt:
Konkretisierung im AVV

- Hinsichtlich der Art der Verarbeitung muss aus der Vereinbarung erkennbar sein, welche Verarbeitungsvorgänge gem. Art. 4 Nr. 2 DSGVO für den konkreten Vertrag relevant sind, siehe auch Tabelle unten.

b) Art der personenbezogenen Daten und Kategorien der von der Verarbeitung betroffenen Personen

3 Anhang B des DPA listet die Arten personenbezogener Daten und die Kategorien der von der Verarbeitung betroffenen Personen auf, die im Rahmen der Nutzung der angebotenen Dienste theoretisch betroffen sein können. In einer AV-Vereinbarung müssen jedoch konkrete Angaben enthalten sein.

[!] ToDo:

- Die Angaben, welche Kategorien personenbezogener Daten welcher betroffenen Personen im Auftrag des Verantwortlichen verarbeitet werden sollen, hat der Verantwortliche in der AV-Vereinbarung einzutragen. Dies kann entweder durch eine Einbeziehung des Ver-

Maßstab: Datenschutzaufsicht

Reicht bei anderen:

2. Art und Zweck der Verarbeitung, Art der Daten sowie Kategorien betroffener Personen

1. **Art und Zweck der Verarbeitung**

   Zweck der Verarbeitung ist die Bereitstellung von virtuellen Konferenzräumen mit Audio/Video-Konferenz, Chat, Dateiaustausch sowie integrierten Planungs- und Dokumentationswerkzeugen.

   Der Auftragnehmer verarbeitet personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO).

   Der Auftragnehmer verpflichtet sich dazu, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Dienstleistungen zu verwenden.

2. **Art der Daten**

   Folgende Daten sind Bestandteil der Datenverarbeitung:

   - Personenstammdaten
   Name oder Pseudonym der Teilnehmer,

   - Kommunikationsdaten der Nutzer der Plattform
   IP-Adressen, Audio/Video-Daten, Chatnachrichten der Teilnehmer,

   - Protokolldaten (Server-Logfiles) der Nutzer der Plattform
   Zugriffskontrolle und -überwachung,

   - Sonstige Daten (Dokumente, Bilder und Grafiken) der Nutzer der Plattform
   von den Teilnehmern hochgeladene oder im virtuellen Konferenzraum erstellte Daten.

Bewertung von Videokonferenzsystemen durch Bln BfDI in 2020/21

🚦	☐ 6	m[redacted]	https://[redacted]	m[redacted] Auftragsverarbeitungs (AV)-Vertrag nach Art. 28 DS-GVO, Version 3 (14.12.2020) [Deutsch]

🚦 Es wurden bei unserer Kurzprüfung keine Mängel gefunden.

Quelle: Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten, v2 (18.02.2021), abrufbar https://**datenschutz.sachsen-anhalt.de**/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Hinweise/2021-BlnBDI-Hinweise_Videokonferenz-Dienste.pdf

Maßstab: Datenschutzaufsicht

Reicht bei anderen:

2. Art und Zweck der Verarbeitung, Art der Daten sowie Kategorien betroffener Personen

1. **Art und Zweck der Verarbeitung**

   Zweck der Verarbeitung ist die Bereitstellung von virtuellen Konferenzräumen mit Audio/Video-Konferenz, Chat, Dateiaustausch sowie integrierten Planungs- und Dokumentationswerkzeugen.

   Der Auftragnehmer verarbeitet personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO).

   Der Auftragnehmer verpflichtet sich dazu, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Dienstleistungen zu verwenden.

2. **Art der Daten**

   Folgende Daten sind Bestandteil der Datenverarbeitung:

   - Personenstammdaten
   Name oder Pseudonym der Teilnehmer,

   - Kommunikationsdaten der Nutzer der Plattform
   IP-Adressen, Audio/Video-Daten, Chatnachrichten der Teilnehmer,

   - Protokolldaten (Server-Logfiles) der Nutzer der Plattform
   Zugriffskontrolle und -überwachung,

   - Sonstige Daten (Dokumente, Bilder und Grafiken) der Nutzer der Plattform
   von den Teilnehmern hochgeladene oder im virtuellen Konferenzraum erstellte Daten.

Reicht beim MS-DPA nicht:

Anhang B – Betroffene Personen und Kategorien personenbezogener Daten

Betroffene Personen: Betroffene Personen sind die Vertreter des Kunden und Endnutzer sowie Angestellte, Auftragnehmer, Mitarbeiter und Kunden des Kunden. Zu den betroffenen Personen können auch Personen gehören, die personenbezogene Daten an Nutzer der von Microsoft bereitgestellten Services übermitteln oder Kontakt zu solchen Nutzern aufnehmen möchten. Microsoft bestätigt, dass sich der Kunde je nach Nutzung der Produkte und Services dafür entscheiden kann, personenbezogene Daten von den folgenden Arten von betroffenen Personen in die personenbezogenen Daten aufzunehmen:

- Mitarbeiter, Auftragnehmer und Zeitarbeitnehmer (derzeitige, ehemalige, zukünftige) des Kunden;
- Angehörige der oben genannten Personen;
- Partner/Kontaktpersonen des Kunden (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeitnehmer von Partnern/Kontaktpersonen (juristische Personen) (derzeitige, ehemalige, zukünftige),
- Benutzer (z. B. Kunden, Klienten, Patienten, Besucher usw.) und andere betroffene Personen, die Benutzer der Dienstleistungen des Kunden sind,
- Partner, Stakeholder oder einzelne Personen, die aktiv mit den Mitarbeitern des Kunden zusammenarbeiten, kommunizieren oder anderweitig interagieren und/oder Kommunikationsmittel wie Anwendungen und Websites verwenden, die vom Kunden bereitgestellt werden;
- Stakeholder oder einzelne Personen, die passiv mit dem Datenexporteur interagieren (z. B. weil sie Gegenstand einer Untersuchung oder Studie sind oder in Dokumenten oder in Korrespondenz mit dem Datenexporteur erwähnt werden);
- Minderjährige Personen; oder
- Berufsgeheimnisträger (z. B. Ärzte, Anwälte, Notare, Kirchenmitarbeiter usw.).

Kategorien von Daten: Die übermittelten personenbezogenen Daten, die in E-Mails, Dokumenten und anderen Daten in elektronischer Form im Rahmen der Produkte und Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung der Produkte und Services die Möglichkeit hat, personenbezogene Daten aus den folgenden Kategorien in die personenbezogenen Daten aufzunehmen:

- Personenbezogene Basisdaten (z. B. Geburtsort, Straßenname und Hausnummer (Adresse), Postleitzahl, Wohnort, Land der Ansässigkeit, Mobiltelefonnummer, Vorname, Nachname, Initialen, E-Mail-Adresse, Geschlecht, Geburtsdatum) einschließlich der personenbezogenen Basisdaten von Familienmitgliedern und Kindern;
- Authentifizierungsdaten (z. B. Benutzername, Kennwort oder PIN-Code, Sicherheitsfrage, Audit-Protokoll);
- Kontaktinformationen (z. B. Adressen, E-Mail-Adressen, Telefonnummern, Social-Media-Kennungen, Notfallkontaktdaten);
- Eindeutige Identifikationsnummern und Signaturen (z. B. Sozialversicherungsnummer, Bankkontonummer, Pass- und Ausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Personalnummer, Studentennummer, Patientennummer, Signatur, eindeutige Kennung bei Tracking-Cookies oder ähnliche Technologien);
- Pseudonymisierte Kennungen;
- Finanz- und Versicherungsinformationen (z. B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartenname und -nummer, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Bonität);
- Geschäftsinformationen (z. B. Kaufverlauf, Sonderangebote, Abonnementinformationen, Zahlungsverlauf);
- Biometrische Informationen (z. B. DNA, Fingerabdrücke und Iris-Erfassungen);
- Standortdaten (z. B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden);
- Fotos, Videos und Audio;
- Internetaktivitäten (z. B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören);
- Geräteidentifikation (z. B. IMEI-Nummer, SIM-Kartennummer, MAC-Adresse);

- Profilierung (z. B. basierend auf beobachteten kriminellen oder antisozialen Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen);
- Personal- und Einstellungsdaten (z. B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen);
- Ausbildungsdaten (z. B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung);
- Staatsbürgerschafts- und Aufenthaltsinformationen (z. B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis);
- Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird;
- Besondere Kategorien von Daten (z. B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Anklagen); oder
- Alle anderen in Artikel 4 DSGVO genannten personenbezogenen Daten.

Die unerwähnte Bombe …

Telekommunikationsrecht

- **Exchange/E-Mail**
- **Videokonferenz**
- **Misch-Dienste (Teams)**
- **Einwahl via Landline („PSTN“)**
- **Zuständigkeit und RGL**

Agenda

- Fokus dieses Vortrags
- Überblick Microsoft-Vertragswerk:
  Product Terms, DPA, EU Data Boundary
- Kritik der Aufsichtsbehörden – was davon ist (noch) berechtigt?
- Zusatzvereinbarung Niedersachsen und andere Rahmenverträge
- Lösungen und Praxis-Tipps
- Copilot
- Meine Wünsche

Zusatzvereinbarungen & RV

- Niedersachsen:
  Teams mit Zusatzvereinbarung im Innenministerium akzeptabel
- „Bundesvertrag“
- Sozialdaten iSd SGB
- Konzern-Zusatzvereinbarungen

… nichts davon ändert die Art der Datenverarbeitung.

… nichts davon in neuer DPA-Fassung.

Berufsgeheimnisträger-Zusatzvereinbarung

- § 203 StGB: Berufsgeheimnisträger Zusatzvereinbarung
  use365.ms/MS203
- Kostenlos (je nach Lizenzweg schwierig)
- m.E. ausreichend, um Strafbarkeit nach § 203 StGB zu vermeiden

Microsoft: Berufsgeheimnisträger Zusatzvereinbarung

use365.ms/MS203

Microsoft

Microsoft Customer Agreement

Berufsgeheimnisträger Zusatzvereinbarung

Diese Berufsgeheimnisträger Zusatzvereinbarung („Zusatzvereinbarung") wird zwischen dem Kunden und der Microsoft Gesellschaft geschlossen, die Parteien des Microsoft Customer Agreement (des „Agreements") sind. Die Parteien sind sich einig, dass diese Zusatzvereinbarung das Agreement ergänzt. Alle Begriffe, die verwendet und nicht definiert werden, sollen dieselbe Bedeutung haben wie im Agreement.

Microsoft ist bewusst, dass der Kunde rechtlichen Verpflichtungen hinsichtlich der Gestattung des Zugriffs auf Informationen von Mandanten des Kunden unterliegt und die Verletzung solcher Verpflichtungen strafrechtliche Folgen für die Beteiligten im Sinne des § 203 StGB (Freiheits-oder Geldstrafe) haben kann.

Microsoft ist gemäß der mit dem Kunden bestehenden Vertragsbestimmungen zur Verschwiegenheit verpflichtet.

Microsoft und Microsofts Subunternehmer dürfen weitere Personen zur Bereitstellung der Onlinedienste einsetzen. Microsoft stellt sicher, dass sowohl die von Microsoft eingesetzten Personen, soweit sie im Zusammenhang mit ihrer Tätigkeit Kenntnis von zur Verfügung gestellten Kundendaten erlangen könnten, als auch die Subunternehmer gemäß der mit dem Kunden bestehenden Vertragsbestimmungen zumindest in Textform zur Verschwiegenheit verpflichtet sind und dass auch die Subunternehmer verpflichtet sind, die von diesen eingesetzten Personen entsprechend zu verpflichten.

Anforderungen § 203 StGB:

- ✓ Formlos möglich
- ✓ Gegenzeichnung nicht erford.
- ✓ Inhalt: Verpflichtung auf „Geheimhaltung" (aber nicht wörtlich nötig)
  Bezugnahme auf § 203 StGB nice, aber nicht erforderlich
- (✓) Verpflichteter? Gesellschaft, nicht mitw. Person.
  Aber Kern ist: „Sorge tragen", nicht Einzelne zu verpflichten.

- ✓ Weitere Personen (Subunternehmer):
  Ist geregelt

LEGAL CHECK
www.legalcheck.digital

Agenda

- Fokus dieses Vortrags
- Überblick Microsoft-Vertragswerk:
  Product Terms, DPA, EU Data Boundary
- Kritik der Aufsichtsbehörden – was davon ist (noch) berechtigt?
- Zusatzvereinbarung Niedersachsen und andere Rahmenverträge
- Lösungen und Praxis-Tipps
- Copilot
- Meine Wünsche

Projektmanagement für M365-Rollout

Out of Scope:

Allgemeine Aspekte wie:
- Rechtsgrundlage für Verarbeitung
- Löschkonzept für E-Mails
- Brillen in Videokonferenz

Verarbeitung in anderen Systemen (außerhalb M365)

Abgrenzen:

- Welche Daten sind wo?
- Was ist führendes System?

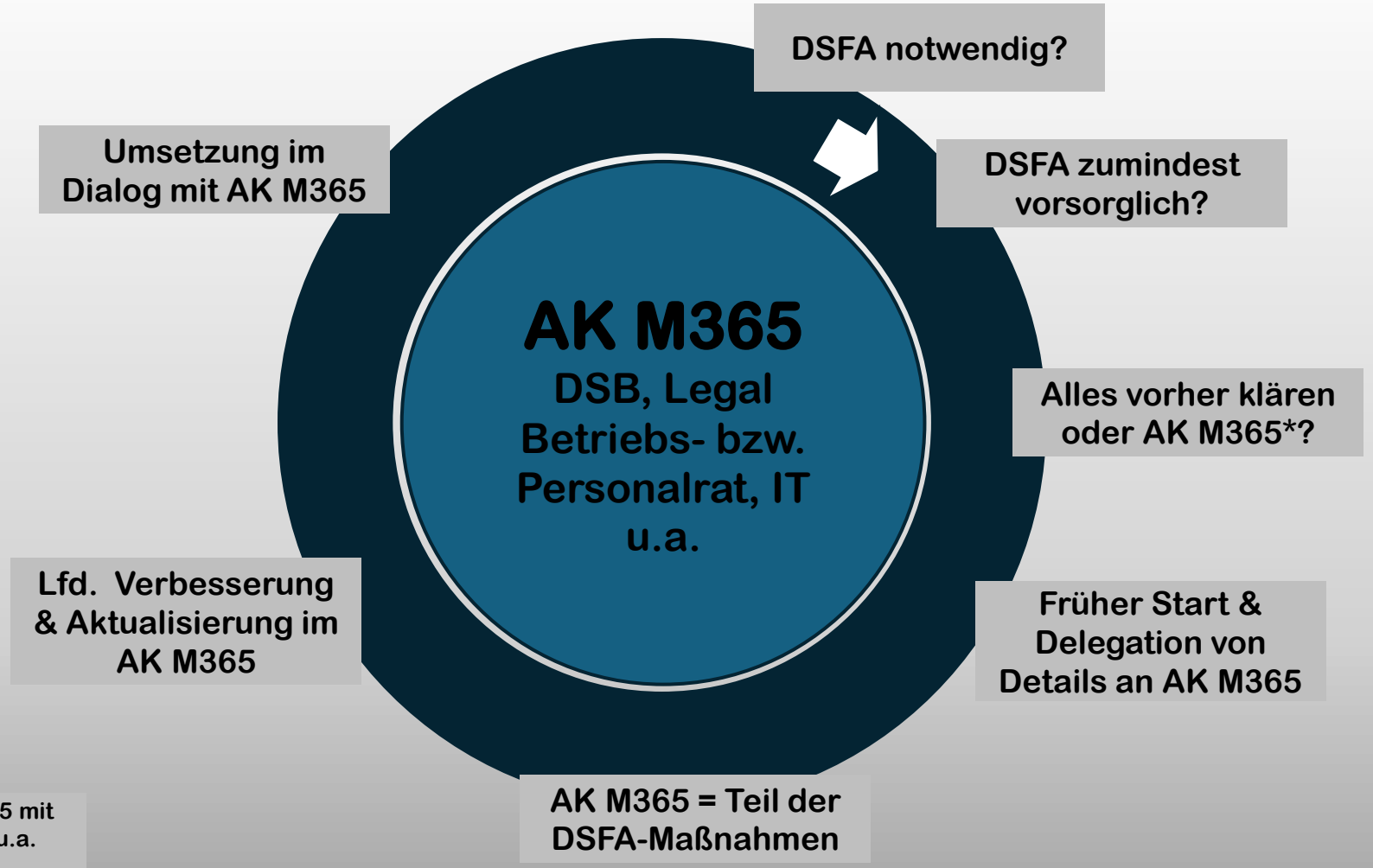
=> Weniger kritisch, wenn Daten nur sporadisch in M365.

In Scope:

Spezifische Fragen von M365:
- US-Cloud
- Microsoft-Verträge
- Kritik von DSK und Aufsichtsbeh.

Konkrete Situation des Kunden, z.B.:
- Regulierung
- Gesundheits-/Sozialdaten, Bankgeheimnis etc.
- Nutzungs-/Anschlusszwang (Behörde, Versorger)
- Jugendliche / Kinder (Schulen)

DSFA nach zwei Jahren nicht fertig?
Delegieren Sie Details und zukünftige Entwicklungen in ein internes M365-Gremium



* AK M365 = Arbeitskreis Microsoft 365 mit DSB, Betriebs- bzw. Personalrat, IT u.a. Siehe folgende Slide

Konkrete Umsetzung in DSFA und BV

Somit setzen sich die im Rahmen dieser DSFA festzulegenden Maßnahmen zusammen aus

- den konkreten Maßnahmen zur Begegnung der bislang festgestellten Risiken (siehe *Zur Risikobegegnung konkret vorgesehene Maßnahmen*, S. 34)

sowie

- einem organisatorischen Prozess, durch den sichergestellt wird, dass die initial ausgesparten sowie die zukünftig hinzukommenden Aspekte und Risiken erfasst werden, der Datenschutzbeauftragte und ggf. weitere Stakeholder rechtzeitig und transparent informiert werden, rechtliche und technische Aspekte behandelt werden und diese DSFA dadurch regelmäßig und angemessen aktualisiert wird, wozu auch die Ergänzung weiterer Maßnahmen gehört. Dies soll durch das (hier und in der Folge so bezeichneten) **„Arbeitskreis M365“** erfolgen, wobei dieser Begriff nicht nur für den Personenkreis, sondern für den gesamten organisatorischen Prozess steht.

7.3.2 *Erfassungs- oder Vorbereitungsphase (Art. 35 Abs. 7 lit. a DSGVO)*

In der ersten Phase der DSFA erfolgt eine systematische Beschreibung der geplanten

Betriebsvereinbarung [Dienstvereinbarung] zum Betrieb von Microsoft 365

(im Folgenden „Betriebsvereinbarung“)

3. Um die mit dem Evergreen-Ansatz verbundenen Neuerungen zu nutzen, aber auch die damit einhergehenden organisatorischen Herausforderungen und Risiken handhaben zu können, vereinbaren die Parteien folgenden Prozess:
   i. Die Arbeitgeberseite und der Betriebsrat vereinbaren eine laufende Abstimmung und Aktualisierung. Hierzu wird der **Arbeitskreis M365** gebildet. Die Mitglieder sollen persönlich benannt werden und dauerhaft am Arbeitskreis teilnehmen.
   ii. Mitglieder des Arbeitskreises sind seitens des Arbeitgebers mindestens:
   [CTO / Leiter M365-Betrieb / Stellvertreter].
   Mitglieder des Arbeitskreises sind seitens des Betriebsrats mindestens:
   [z.B. BR-Vorsitzender oder Stellv.; IT-Zuständiger im Betriebsrat.]
   Weitere Mitglieder sind:
   Die/der Datenschutzbeauftragte und sowie die/der [CISO/IT-Sicherheitsbeauftragte; in

Checkliste

- Rechtliches: Ihre Position zu DSK?
- Wofür nutzen Sie M365?
- Lizenzen, Bezugswege, Zusatzvereinbarungen, Compliance-Tools etc.
- Alles „in M365“: Mal eben die Einstellungen (800+)
  Tipp: Center for Internet Security (CIS)
  https://www.cisecurity.org/benchmark/microsoft_365
  Level 1 meist ausreichend
- Alles „über und unter“ M365:
  - Global Admins,
  - organisatorische Anweisungen; FAQ
  - Roll-out und Schulungskonzept

Agenda

- Fokus dieses Vortrags
- Überblick Microsoft-Vertragswerk:
  Product Terms, DPA, EU Data Boundary
- Kritik der Aufsichtsbehörden – was davon ist (noch) berechtigt?
- Zusatzvereinbarung Niedersachsen und andere Rahmenverträge
- Lösungen und Praxis-Tipps
- Copilot
- Meine Wünsche

~~Copilot~~
Die Copilot-Varianten

- Welcher Copilot:
  Copilot Chat (ehemals Bing, ohne M365) vs. „Microsoft 365 Copilot“
- Wie eingeloggt (bei Copilot Chat)? EU Data Boundary
- Was ist das Besondere an Microsoft 365 Copilot?

3. Halten Sie das Team auf dem Laufenden

Verwenden Sie Copilot in Teams, um wichtige Besprechungen zusammenzufassen, die häufigsten Fragen und Aktionspunkte der Besprechung zu identifizieren. Verwenden Sie Copilot in Word, um ein erstes FAQ-Dokument zu erstellen.

Copilot in Teams | Copilot in Word

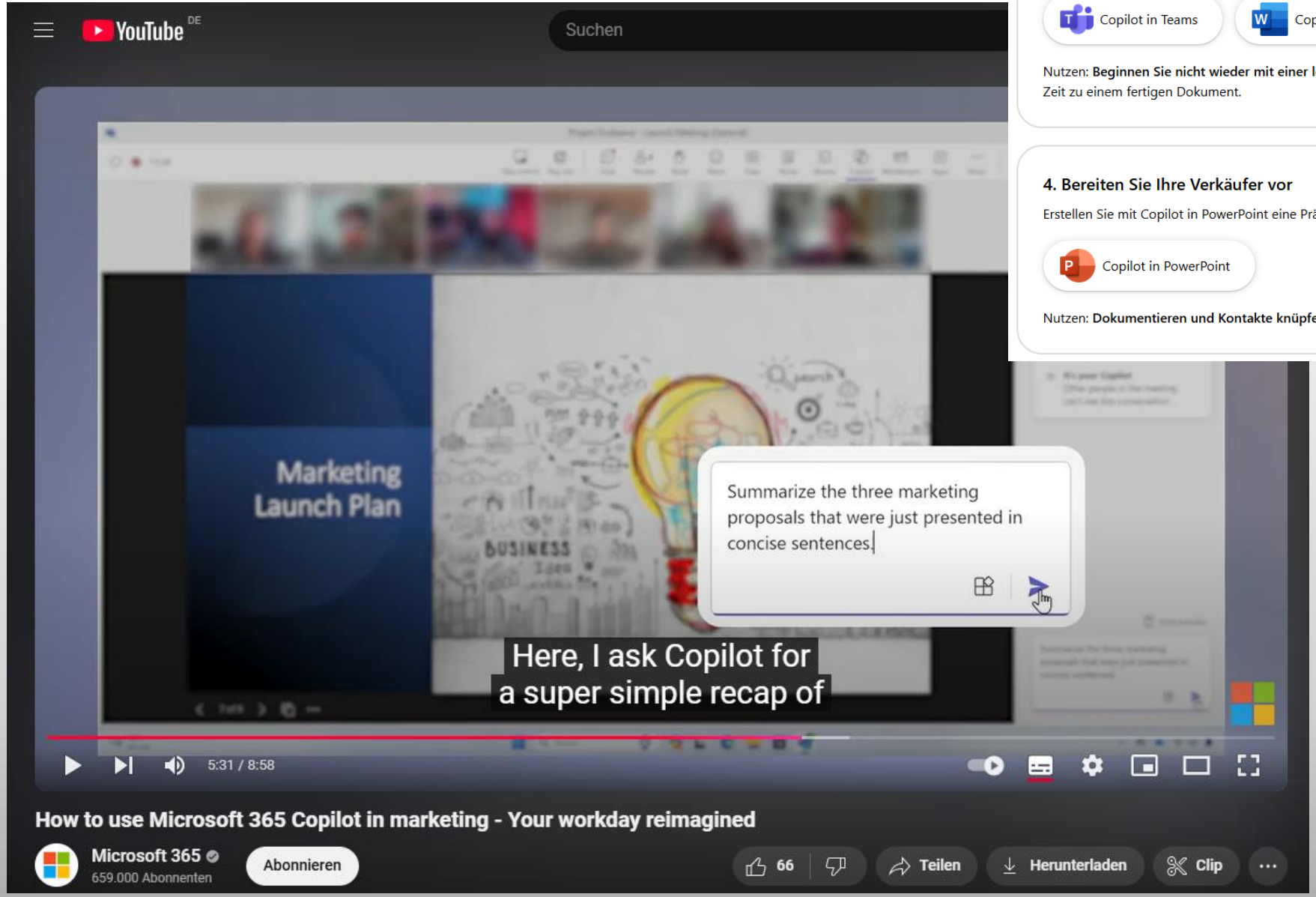
Nutzen: **Beginnen Sie nicht wieder mit einer leeren Seite**. Erstellen Sie mit Copilot einen Entwurf und gelangen Sie in einem Bruchteil der Zeit zu einem fertigen Dokument.

4. Bereiten Sie Ihre Verkäufer vor

Erstellen Sie mit Copilot in PowerPoint eine Präsentation aus Ihrem Marketingplan, um sie mit Ihrem Vertriebsteam zu teilen.

Copilot in PowerPoint

Nutzen: **Dokumentieren und Kontakte knüpfen** Ihr Plan, Verkäufer auf dem Laufenden zu halten.



Wofür nutzen Sie Copilot?

- „Keine pbD“ => mit unsensiblen Daten geht alles

- Risiko? Clustern Sie die Nutzung
  - Unsensible Daten: OK – ähnlich Suchmaschine
  - Use cases medium: Richtlinien
  - Kritisch: Individuell prüfen & freigeben

Muster für AI-Richtlinie

11.4.1 Use Case 1: Unkritische Daten

Unkritisch ist es aus datenschutzrechtlicher Sicht zunächst, wenn Daten ohne Personenbezug in ein LLM gegeben werden. Aus Perspektive der Informationssicherheit ist freilich eine breitere Betrachtung der Frage erforderlich, welche Daten als unkritisch angesehen werden; auch Daten ohne Personenbezug können sehr vertrauliche und geheimhaltungsbedürftige Informationen enthalten.

Häufig wird behauptet, nur Daten ohne jeglichen Personenbezug dürften ohne nähere Prüfung in ein LLM gegeben werden. Richtig ist jedoch, dass auch personenbezogene Daten mit einem unkritischen Risiko – hier verkürzt und datenschutzrechtlich unkorrekt als „unkritische Daten" bezeichnet – für Prompts und ähnliche Zwecke (wie etwa als zusätzliche Daten im Rahmen von Retrieval Augmented Generation (RAG)) verwendet werden dürfen. Hierbei handelt es sich vor allem um öffentlich verfügbare Informationen sowie ähnlich unkritische Konstellationen, von den Zwecken her betrachtet dient die Verarbeitung häufig internen Recherchen, journalistischen, literarischen oder humoristischen Zwecken.

11.4.2 Use Case 2: Mittelkritische Daten

Um KI ernsthaft zu nutzen, wird die Nutzung in aller Regel über ChatGPT oder Microsoft Copilot in der Variante ohne Anmeldung hinausgehen, und dabei werden meist auch im größeren Umfang Daten einbezogen werden, die aus Sicht von Datenschutz und Informationssicherheit größere Relevanz haben als in der vorherigen Fallgruppe der „unkritischen Daten".

Dabei soll die Nutzung durch Microsoft 365 Copilot betrachtet werden. Wie oben dargestellt gilt für den Core Service das DPA mit der AVV und weiteren Zusagen. Datenschutzrechtlich werden die vom Nutzer eingegebenen Daten also nicht an einen Dritten übermittelt, sondern lediglich im Auftrag verarbeitet. Der Verantwortliche benötigt also „lediglich" eine Rechtsgrundlage für die eigene Verarbeitung.

11.4.2.1 Spezifische Risiken beim Microsoft 365 Copilot

Mehrwert und Gefahr der M365-Copiloten liegen darin, dass der Copilot auf Daten zugreifen kann, auf die der Nutzer im Rahmen seines M365-Accounts Zugriff hat. Dies ist sehr nützlich, wenn es sich um datenschutzrechtlich wenig kritische Daten handelt, etwa frühere Produktpräsentationen für potenzielle Kunden. Hieraus können ohne datenschutzrechtliches Risiko neue Produktpräsentationen erstellt werden, die auch neue Informationen wie eine aktuelle Preisliste einbinden.

Agenda

- Fokus dieses Vortrags
- Überblick Microsoft-Vertragswerk:
  Product Terms, DPA, EU Data Boundary
- Kritik der Aufsichtsbehörden – was davon ist (noch) berechtigt?
- Zusatzvereinbarung Niedersachsen und andere Rahmenverträge
- Lösungen und Praxis-Tipps
- Copilot
- Meine Wünsche

An die Aufsichtsbehörden: Eine
einheitliche,
aktuelle,
maßvolle
Bewertung

An Microsoft: Eine
einheitliche
Regelung
ohne Specials in
Zusatzvereinbarungen.

(Und Ziffern im DPA.)

Dr. Olaf Koglin
Rechtsanwalt,
Geschäftsführer LegalCheck

Vielen Dank für Ihr Interesse!