LEGAL CHECK
Approval as a Service



Dr. Olaf Koglin
Rechtsanwalt,
Geschäftsführer LegalCheck

Microsoft Teams: Aufzeichnungen, Transkription & Co.

Dr. Olaf Koglin
LegalCheck 365 GmbH
IHK Offenbach, 04.11.2026

Nachtrag:
URLs aus dem Webinar

Neue Fassung des Data Protection Addendum (DPA) von Microsoft v. 01.11.2026:

- Übersicht alle DPA-Fassungen (Microsoft): use365.ms/DPA
- Analyse & Infos dazu auf www.legalcheck.de/blog/dpa-2026-11-01
- **Webinar am Di 10.11.2026 11-12 Uhr mit Johannes Nehlsen und Olaf Koglin**
  Kostenlose Anmeldung unter use365.ms/NovemberDPA

Informationen zur Webinarreihe M365-Club von LegalCheck:

- use365.ms/M365-Club

LEGAL CHECK
www.legalcheck.digital

Noch mehr aktuelles M365-Wissen

use365.ms/M365-Club

- Ein Jahr M365-Club für
  für 860,- EUR pa (ne.)
- Zwei Webinare je Monat (mind.)
- Die nächsten 3 Termine zu Teams, Dokumentation und Texten
- Einfach anmelden auf
  use365.ms/M365-Club



Dom Côté
Gründer SoloPro
Ex-Microsoft
M365-Experte für KMU



Carolin Loy
Bereichsleitung
Digitalwirtschaft und
Rechtsfragen KI, BayLDA



Dr. Olaf Koglin
Rechtsanwalt
Geschäftsführer
LegalCheck



Johannes Nehlsen
Oberregierungsrat, Universität Würzburg
Stabsstelle IT-Recht des Digitalverbunds
Bayern im Hochschulbereich

LEGAL CHECK
Approval as a Service

Microsoft 365 & Copilot
Datenschutz und Sicherheit

2x monatlich
Webinar plus
Aufzeichnungen,
Dokumente &
Community

- Datenschutz bei M365 und Copilot
- AI Act und angrenzende Rechtsgebiete
- IT-Sicherheit und Einstellungen
- Updates und Best Practices von M365-Experten
- Zusatz-Sessions mit Special Guests
- Konkrete Tipps und Lösungen

legalcheck.de/m365-club

Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026



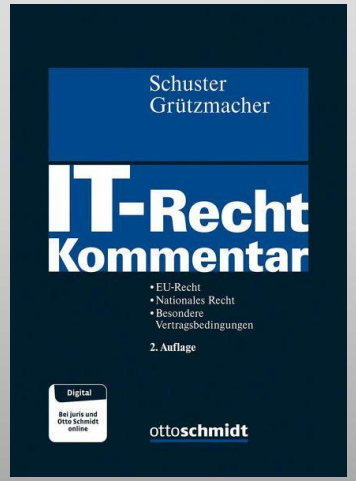
- **Vortrag: Aufzeichnung und Transkription bei Teams**
  - **Teams und Zusatzfunktionen**
  - **Rechtsgrundlage(n)**
  - **Folgen bei Berechtigtem Interesse**
  - **Pop-Ups und Einbindung von Hinweisen**
  - **§ 201 StGB**
  - **Dokumentation: VVT, DSE, DSFA-Ergänzung**

- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital







Über Olaf Koglin



Dr. Olaf Koglin
Rechtsanwalt,
Geschäftsführer LegalCheck

- IT-Recht seit 1996
- Promotion über Open Source Software

- 20+ Jahre Berufserfahrung u.a. bei Capgemini, Accenture, Axel Springer und als Prokurist von upday

- Gründung von LegalCheck 2021

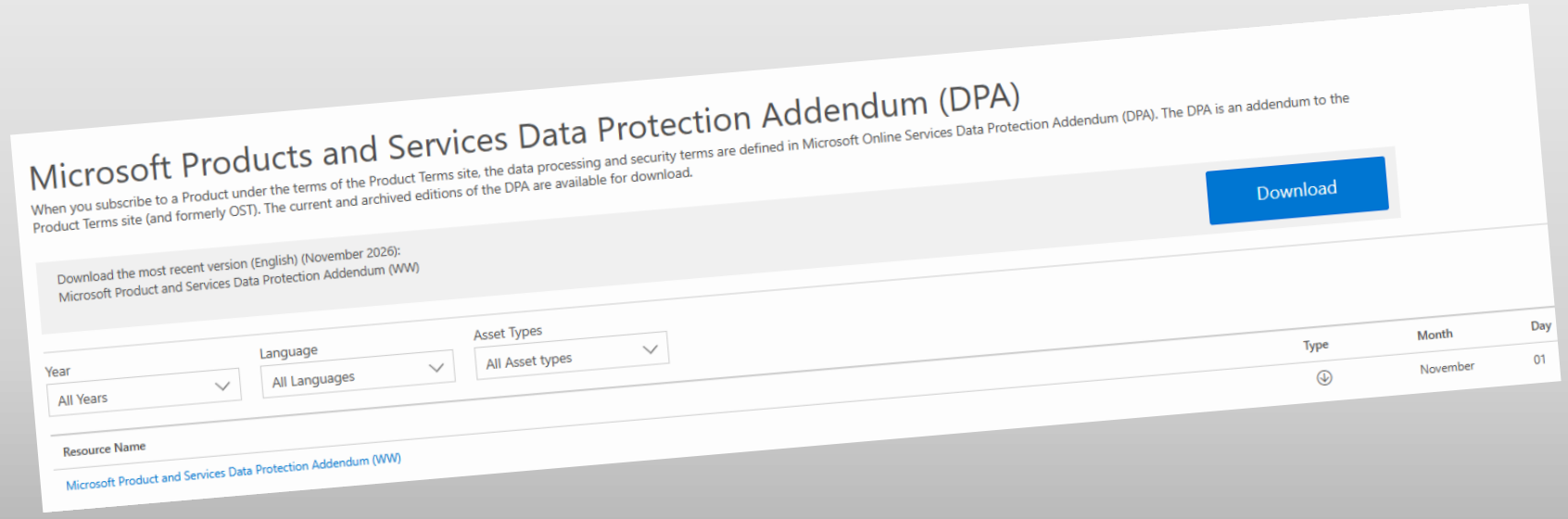
- Datenschutz (Auswahl):
  - Beirat der Fachzeitschrift Datenschutz-Berater
  - Autor u.a. im Beck‘schen Formularhandbuch Datenschutzrecht seit 1. Aufl. 2014 & im Beck‘schen Handbuch Konzerndatenschutz
  - Referent auf zahlreichen Kongressen, u.a. Chaos Computer Club, DGRI/DSRI, Datenschutz-Konferenz und bei Verbänden
  - Gastspeaker in Podcasts und bei Events

LEGAL CHECK
www.legalcheck.digital

+++ AKTUELL: DPA-Ergänzung +++

use365.ms/DPA

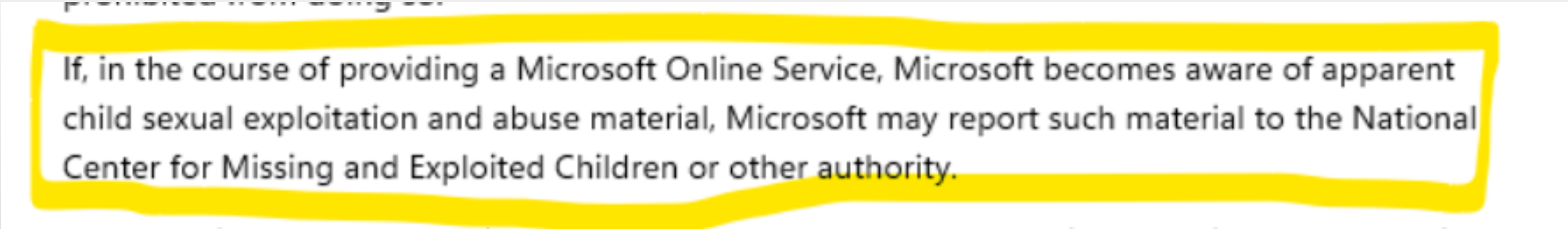
- Das DPA ist das Dokumente für Microsoft 365 und weitere Online Services, in dem Datenschutz und weitere Themen geeregelt werden.
- Unregelmäßig – meist 1-3 mal je Jahr – erscheinen neue Fassungen mit verschieden großen Änderungen.
- Am 01.11.2026 erschien eine neue Fassung:



LEGAL CHECK
www.legalcheck.digital

Microsoft-DPA vom 01.11.2026:

Ergänzung in Kapitel „Disclosure of Processed Data“:



If, in the course of providing a Microsoft Online Service, Microsoft becomes aware of apparent child sexual exploitation and abuse material, Microsoft may report such material to the National Center for Missing and Exploited Children or other authority.

LEGAL CHECK
www.legalcheck.digital

Fragen und Antworten dazu

- Unklare Klauseln („any other authority“)
- AVV-Weisungsgebundenheit vs. Meldung nach Art. 28 Abs. 3 lit. a DSGVO
- DE-/Unionsrecht vs. US-Recht
- DSGVO vs. Art. 7, 18 DSA

Mehr dazu auf www.legalcheck.de/blog/dpa-2026-11-01

Webinar am Di 10.11.2026 11-12 Uhr mit Johannes Nehlsen und Olaf Koglin
Kostenlose Anmeldung unter use365.ms/NovemberDPA

LEGAL CHECK
www.legalcheck.digital

Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026



- **Vortrag: Aufzeichnung und Transkription bei Teams**
  - **Teams und Zusatzfunktionen**
  - **Rechtsgrundlage(n)**
  - **Folgen bei Berechtigtem Interesse**
  - **Pop-Ups und Einbindung von Hinweisen**
  - **§ 201 StGB**
  - **Dokumentation: VVT, DSE, DSFA-Ergänzung**

- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital

- **Der erste Termin unserer Reihe zu**
  Teams: Rechtsgrundlagen, Einstellungen und Texte zu Videoaufzeichnung, Transkription& Übersetzung
  Teil 1 mit Carolin Loy
  ist nun am Fr. 13.11. von 11- 12 Uhr (Freitag dem 13!)
- Davor sind:
  - **Di 10.11.2026, 11-12 Uhr:** Sonder-Termin zu den **DPA-Änderungen mit Johannes Nehlsen** (siehe oben), Anmeldung über use365.ms/NovemberDPA
  - **Mi 11.11.2026, 11-12 Uhr:** Special zu **M365 und Sozialdatenschutz (SGB), wo ich Josefin Burk von der BGHW** ganz herzlich begrüße. Im aktuellen Heft des Datenschutz-Beraters gibt es einen Artikel von uns beiden zu dem Thema. Hier haben wir die Gelegenheit, das Thema ausführlicher zu erläutern und auf Fragen einzugehen.
- **Mi 18.11. 11-12 Uhr:** Regulärer Termin des M365-Clubs mit dem **2. Teil zu Teams; Fokus auf öffentlichen Stellen (aka: "kein berechtigtes Interesse als RGL") und § 201 StGB**
- **Mi 25.11. 10:00 - 11:30: KI-Fachkunde im November**, diesmal mit **Prof. Dr. Alexander Golland**
- **Mi 02.12. 11-12 Uhr:** Regulärer Termin des M365-Clubs mit dem **3. und abschließenden Teil zu Teams: Einstellungen, Mustertexte und was man sonst noch braucht** (Abwägung und Dokumentation des berechtigten Interesses, VVT, ggf. DSFA).
- **Mi 16.12. 11-12 Uhr:** Regulärer Termin des M365-Clubs

Bitte habt Verständnis für die zahlenreichen unplanmäßigen Termin und Verschiebungen. Und wie immer: Sollte Microsoft das DPA erneut ändern/korrigieren, das DPF gekippt werden oder Ähnliches passieren, werden wir die Planung erneut umstellen.

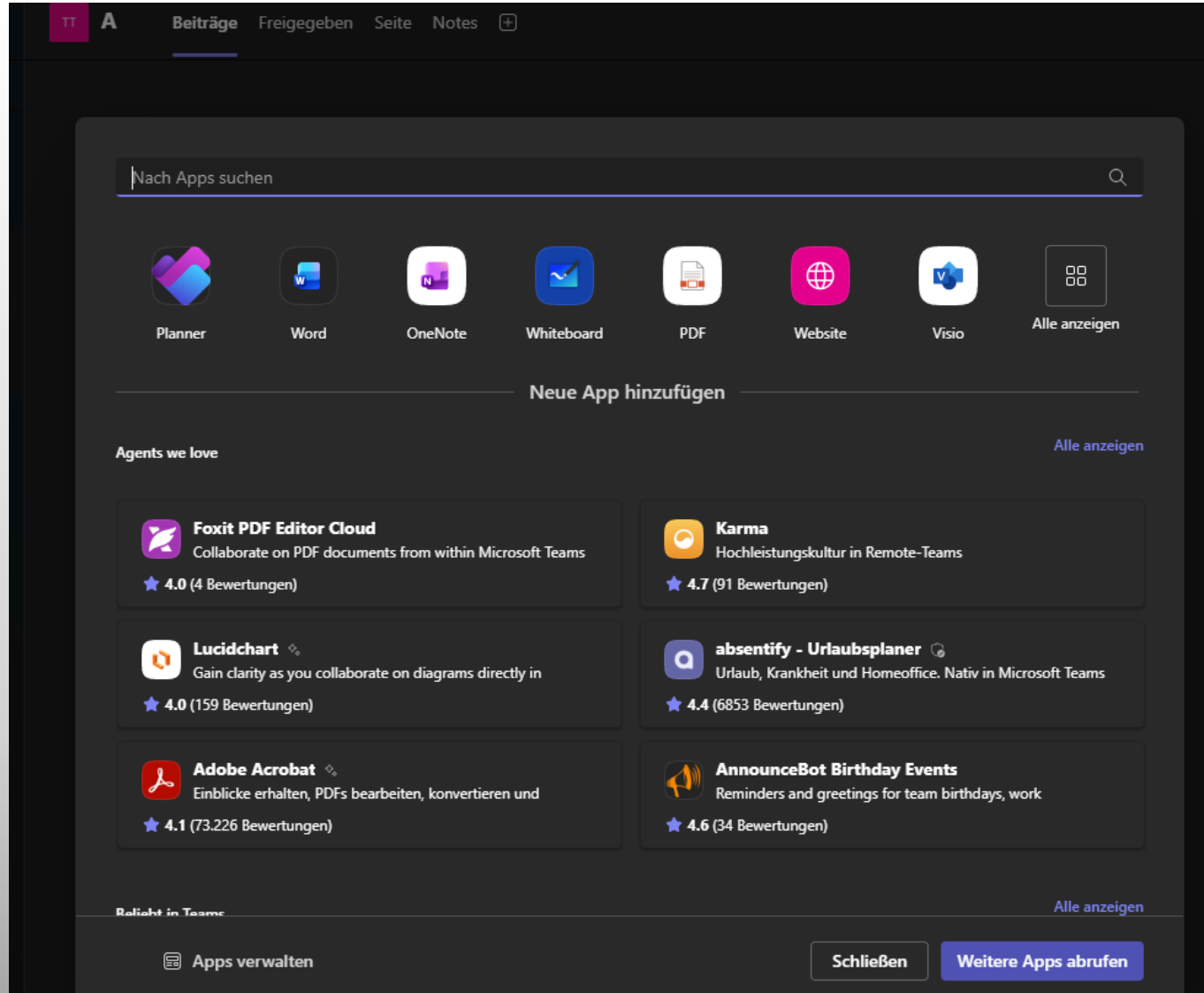
Hier nun die Zusammenfassung zur DPA-Änderung:
Weitergabe von Daten beim Verdacht auf Material zu Kindesmissbrauch: Sind die Änderungen im DPA mit unserem Recht vereinbar?
Was ist passiert?
👉 Microsoft hat am 01.11. eine neue Fassung seines DPA bekanntgegeben.
👉 Darin ist die entsprechende Einfügung, die Microsoft das Recht gibt, solche Materialien zu melden
👉 An wen gemeldet werden kann, ist nicht klar umrissen
👉Weisungsgebundenheit der AVV versus Pflicht zur Meldung, DSGVO und weiteres EU-Recht versus **18 U.S.C. § 2258D** mit US-Institutionen

Was sind die Fragen und Probleme?
🚨 Für wen gilt die neue DPA-Fassung? Siehe dazu die bekannte Klausel im DPA zu Nach- und Neulizenzierungen, ggf. überlagert durch Zusatzvereinbarungen mit Microsoft
🚨 Art. 7 DSA zu Maßnahmen der Provider zur Erkennung rechtswidriger Inhalte
🚨 Meldepflicht nach Art. 18 DSA; Gefahrenabwehr versus Strafverfolgung bei Bestandmaterial
🚨 Was ist "Material" - auch Texte mit Betroffenen- und Arztberichten.
🚨 Welche Bereiche von M365 unterliegen Telekommunikations- / ePrivacy-Recht, wann ist man im der allgemeinen DSGVO?
🚨 Anpassungen bei DSFA und Datenschutzhinweisen?

Von welchem Teams sprechen wir?

Teams besteht aus:

- Videokonferenzen
- Collaboration
- Einbindung von Dateien u.v.m.
- Einbindung von Apps etc.



Sonderfunktionen in Teams-Videokonferenzen

- Besondere Rechte (Referenten / Präsentieren)
- Reaktion / Applaus
- Aufzeichnung des Videos
- Untertitel (nur vorübergehend)
- Transkription (dauerhaftes Wortprotokoll mit „äähm“) und Facilitator (KI-Zusammenfassungen statt wörtlichem Protokoll)

LEGAL CHECK
www.legalcheck.digital

Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026

- Vortrag: Aufzeichnung und Transkription bei Teams
  - Teams und Zusatzfunktionen
  - Rechtsgrundlage(n)
  - Folgen bei Berechtigtem Interesse
  - Pop-Ups und Einbindung von Hinweisen
  - § 201 StGB
  - Dokumentation: VVT, DSE, DSFA-Ergänzung

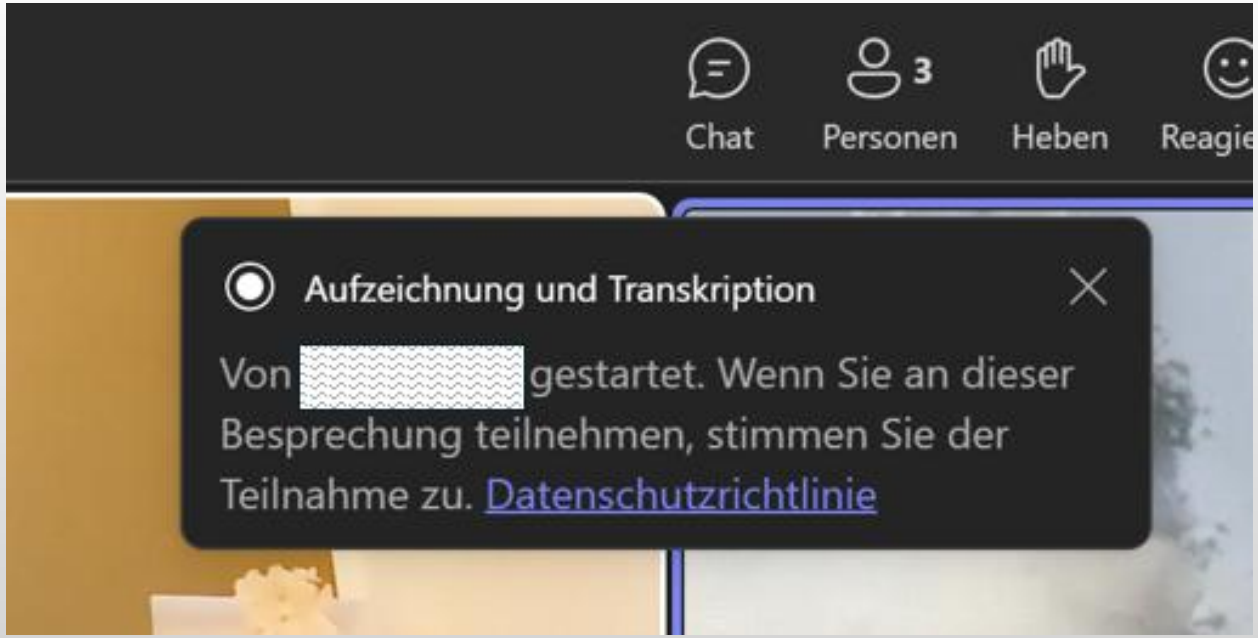
- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital



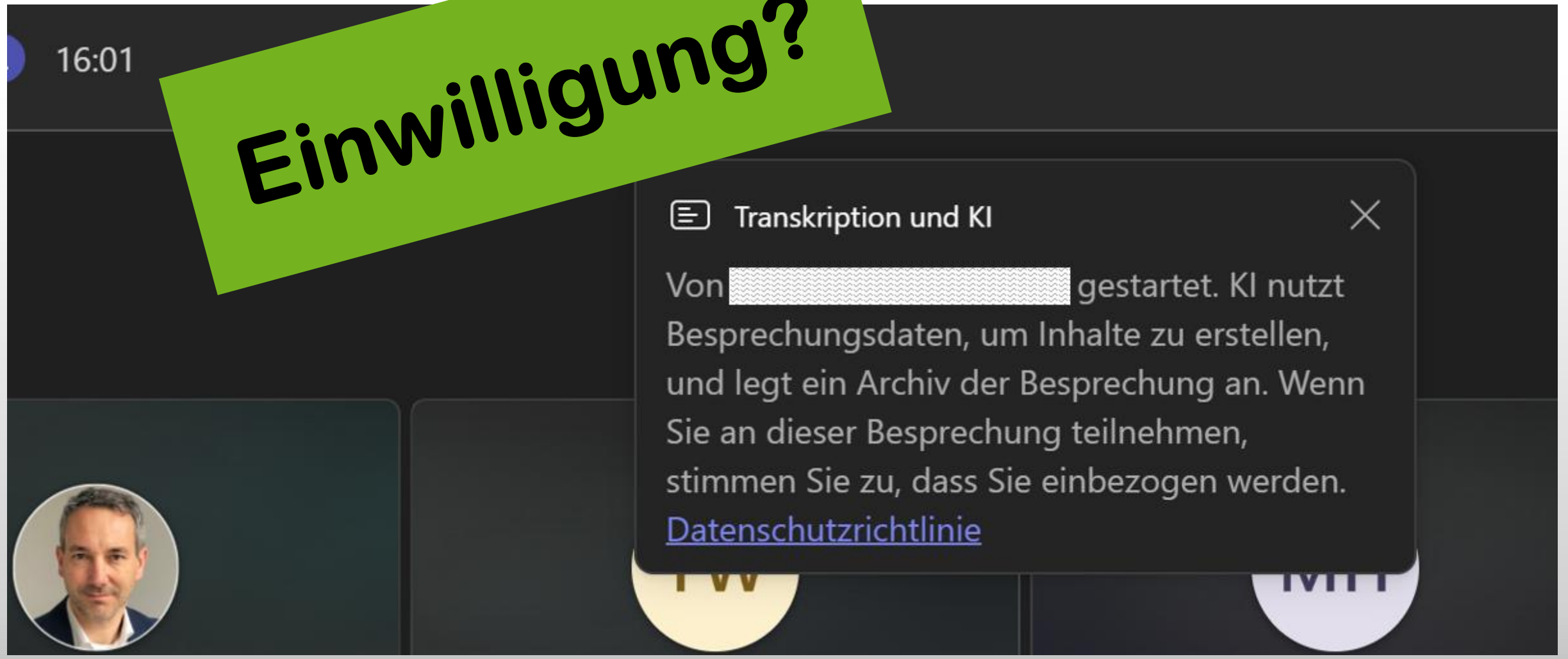
www.legalcheck.digital

Aus Sicht der Teilnehmenden:



LEGAL CHECK
www.legalcheck.digital

Einwilligung?



LEGAL CHECK
www.legalcheck.digital

Mögliche Rechtsgrundlagen

bestes Angebot:

Einwilligung (lit. a)	Vertrag (lit. b)	„berechtigtes Interesse“
Vorteile: ▪ Frei vereinbar Nachteile: ▪ Strenge Anforderungen ▪ Widerrufbar (Art. 7 Abs. 3 DSGVO)	Vorteile: ▪ Super (sofern anwendbar) Nachteile: ▪ Nur mit Vertragspartner ▪ Nicht mit MA des Kunden etc.	Vorteile: ▪ Sehr flexibel Nachteile: ▪ Abwägung: Verschiedene Meinungen ▪ Widerspruchsrecht & Hinweis (Art. 21 DSGVO) ▪ Bürokratie und EuGH-RSpr. (rechtzeitige Information über die Interessen, Abwägung & Dokumentation)

LEGAL CHECK
www.legalcheck.digital

Empfehlung für die RGL:

Berechtigtes Interesse. Dafür erforderlich:

- Abwägung und Dokumentation (EuGH, EDSA-Leitlinien):
  - Welches berechtigtes („legitimes“) Interesse?
  - Erforderlichkeit (kein milderes Mittel)
  - Interessenabwägung; ggf. Schutzmaßnahmen

- Ergebnis Rahmen der Abwägung: Keine Aufzeichnung etc. bei Bewerbungsgesprächen, BEM etc.
  Ausnahme: Hörgeschädigte, Art. 26 vs. Art. 8 EU-GRCh
  Ggf. Policy / Schulung

- Rechtzeitig (!) informieren

- Widerspruchsrecht gem. Art. 21 Abs. 1 DSGVO,
  getrennter Hinweis nach Art. 21 Abs. 4 DSGVO !

LEGAL CHECK
www.legalcheck.digital

Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026

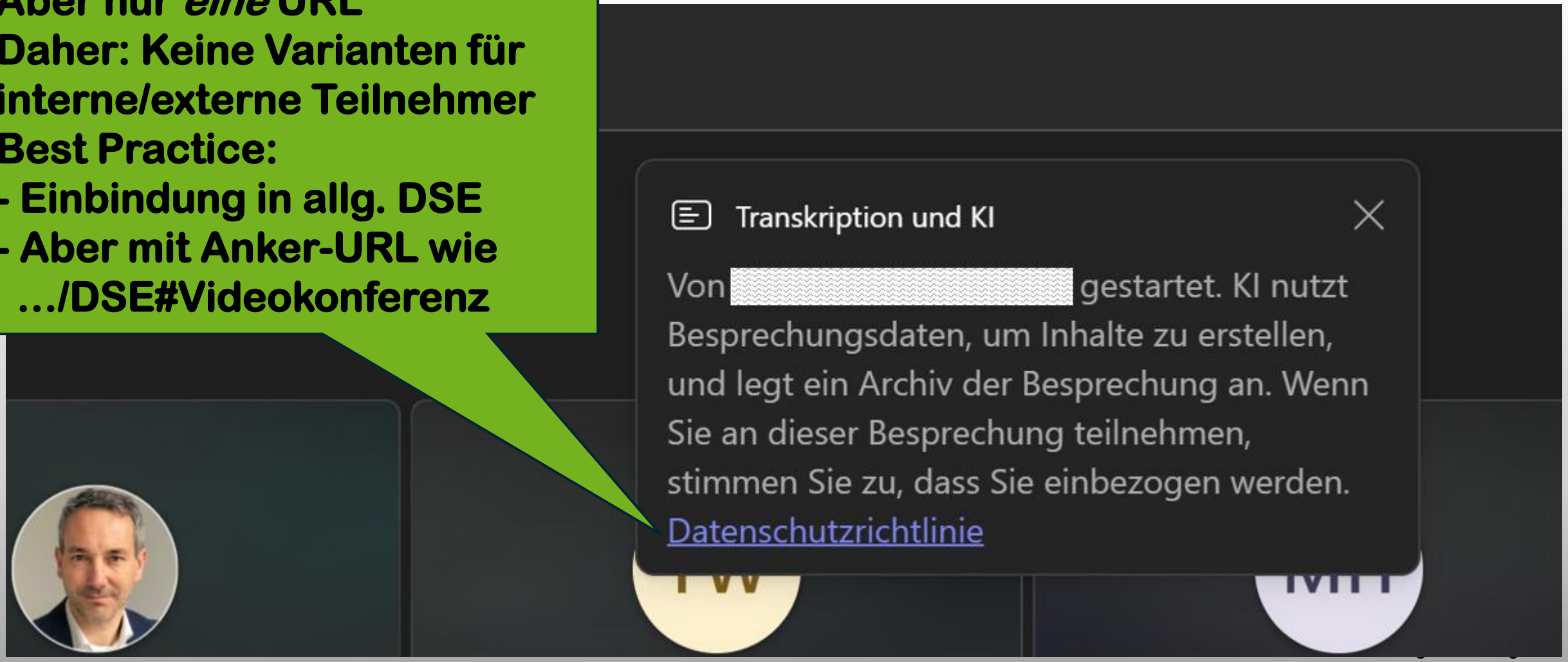
- Vortrag: Aufzeichnung und Transkription bei Teams
  - Teams und Zusatzfunktionen
  - Rechtsgrundlage(n)
  - Folgen bei Berechtigtem Interesse
  - Pop-Ups und Einbindung von Hinweisen
  - § 201 StGB
  - Dokumentation: VVT, DSE, DSFA-Ergänzung

- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital

Spielräume in Teams:

- **Angabe eigener URL für Datenschutzhinweise**
- **Aber nur *eine* URL**
- **Daher: Keine Varianten für interne/externe Teilnehmer**
- **Best Practice:**
  - Einbindung in allg. DSE
  - Aber mit Anker-URL wie …/DSE#Videokonferenz



Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026

- Vortrag: Aufzeichnung und Transkription bei Teams
  - Teams und Zusatzfunktionen
  - Rechtsgrundlage(n)
  - Folgen bei Berechtigtem Interesse
  - Pop-Ups und Einbindung von Hinweisen
  - § 201 StGB
  - Dokumentation: VVT, DSE, DSFA-Ergänzung

- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital

Achtung, Strafrecht!

§ 201
Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) [1]Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

LEGAL CHECK
www.legalcheck.digital

Achtung, Strafrecht!

- Liegt TB-Merkmal auf „Tonträger aufnimmt“ vor, wenn nur „on the fly“ verarbeitet wird?
  Meinung: bei Untertitel nicht
  Aber bei Speicherung

- TB-Merkmal „unbefugt“:
  DSGVO und StGB nicht einheitlich
  StGB hat niedrigere Anforderungen an Rechtsgutverzicht
  Hinweise iVm Teilnahme könnten (!) ausreichen

- „unbefugt“ als Tatbestand, nicht rechtliche Bewertung: Dann Erlaubnistatbestandirrtum. § 16 Abs. 1 StGB => Vorsatz entfällt
  Anders bei falscher rechtlicher Einschätzung (vgl. § 17 StGB)

§ 201
Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) [1]Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

LEGAL CHECK
www.legalcheck.digital

Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026

- Vortrag: Aufzeichnung und Transkription bei Teams
  - Teams und Zusatzfunktionen
  - Rechtsgrundlage(n)
  - Folgen bei Berechtigtem Interesse
  - Pop-Ups und Einbindung von Hinweisen
  - § 201 StGB
  - Dokumentation: VVT, DSE, DSFA-Ergänzung

- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital

Texte und Dokumentation

Berechtigtes Interesse. Dafür erforderlich:

- Textbausteine für Datenschutzhinweise (in Haupt-DSE) mit Benennung aller berechtigten Interessen sowie Widerspruchsrecht
- Ergebnis Rahmen der Abwägung: Keine Aufzeichnung etc. bei Bewerbungsgesprächen, BEM etc.
  Ausnahme: Hörgeschädigte, Art. 26 vs. Art. 8 EU-GRCh
- Dokumentation der Abwägung sowie VVT und ggf. DSFA-Ergänzung
- Ggf. Policy / Schulung

LEGAL CHECK
www.legalcheck.digital

Take-Away

Untertitel, Transkription und Aufnahme sind in den meisten Fällen möglich – mit folgenden Mitteln:

- **RGL meist berechtigtes Interesse.**
- **Team-Features für „Einwilligung“ wird nur technisch genutzt, um Transparenz herzustellen**
- **Rechtzeitig informieren: Bereits in Teams-Einladung**
- **EINE URL und EIN Dokument mit Datenschutzhinweisen**
- **Ausnahme: Hörgeschädigte, Art. 26 vs. Art. 8 EU-GRCh**
  Ggf. Policy / Schulung
- **Widerspruchsrecht & Dokumentation beachten**

LEGAL CHECK
www.legalcheck.digital

Die heutige Agenda

- Herzlich Willkommen
  - Über mich
  - Aktuell: Probleme mit dem neuen Microsoft-DPA vom 01.11.2026

- Vortrag: Aufzeichnung und Transkription bei Teams
  - Teams und Zusatzfunktionen
  - Rechtsgrundlage(n)
  - Folgen bei Berechtigtem Interesse
  - Pop-Ups und Einbindung von Hinweisen
  - § 201 StGB
  - Dokumentation: VVT, DSE, DSFA-Ergänzung



- Fragen & Diskussion

LEGAL CHECK
www.legalcheck.digital

LEGAL
CHECK
www.legalcheck.digital

Noch mehr aktuelles M365-Wissen

use365.ms/M365-Club

- Ein Jahr M365-Club für
  für 860,- EUR pa (ne.)
- Zwei Webinare je Monat (mind.)
- Die nächsten 3 Termine zu Teams, Dokumentation und Texten
- Einfach anmelden auf
  use365.ms/M365-Club



Dom Côté
Gründer SoloPro
Ex-Microsoft
M365-Experte für KMU



Carolin Loy
Bereichsleitung
Digitalwirtschaft und
Rechtsfragen KI, BayLDA



Dr. Olaf Koglin
Rechtsanwalt
Geschäftsführer
LegalCheck



Johannes Nehlsen
Oberregierungsrat, Universität Würzburg
Stabsstelle IT-Recht des Digitalverbunds
Bayern im Hochschulbereich

LEGAL CHECK
Approval as a Service

Microsoft 365 & Copilot
Datenschutz und Sicherheit

2x monatlich
Webinar plus
Aufzeichnungen,
Dokumente &
Community

- Datenschutz bei M365 und Copilot
- AI Act und angrenzende Rechtsgebiete
- IT-Sicherheit und Einstellungen
- Updates und Best Practices von M365-Experten
- Zusatz-Sessions mit Special Guests
- Konkrete Tipps und Lösungen

legalcheck.de/m365-club

Und nicht vergessen:

Neues DPA von Microsoft:

Mehr dazu auf www.legalcheck.de/blog/dpa-2026-11-01

Webinar am Di 10.11.2026 11-12 Uhr mit Johannes Nehlsen und Olaf Koglin
Kostenlose Anmeldung unter use365.ms/NovemberDPA

LEGAL CHECK
www.legalcheck.digital



Dr. Olaf Koglin
Rechtsanwalt,
Geschäftsführer LegalCheck

Sie haben noch Fragen?
Wir unterstützen Sie gerne.

ok@legalcheck.digital | www.legalcheck.digital

Back-up

LEGAL CHECK
www.legalcheck.digital

Wie hilft LegalCheck?



Kunde:
Will M365 einführen.

Das Projekt stockt, weil spezielle Kenntnisse zum Datenschutz bei M365 fehlen.

Der Datenschutzbeauftragte, BR oder Vorstand hat noch Bedenken.

Niemand erstellt eine Datenschutz-Folgenabschätzung.

LegalCheck: Kennt genau diese Lage bei seinen Kunden.

Hat die Kenntnis zum Datenschutz bei M365.

Kennt die Bedenken und wie man sie löst. Weiß, wann man statt über Datenschutzrecht über Projektmanagement sprechen sollte.

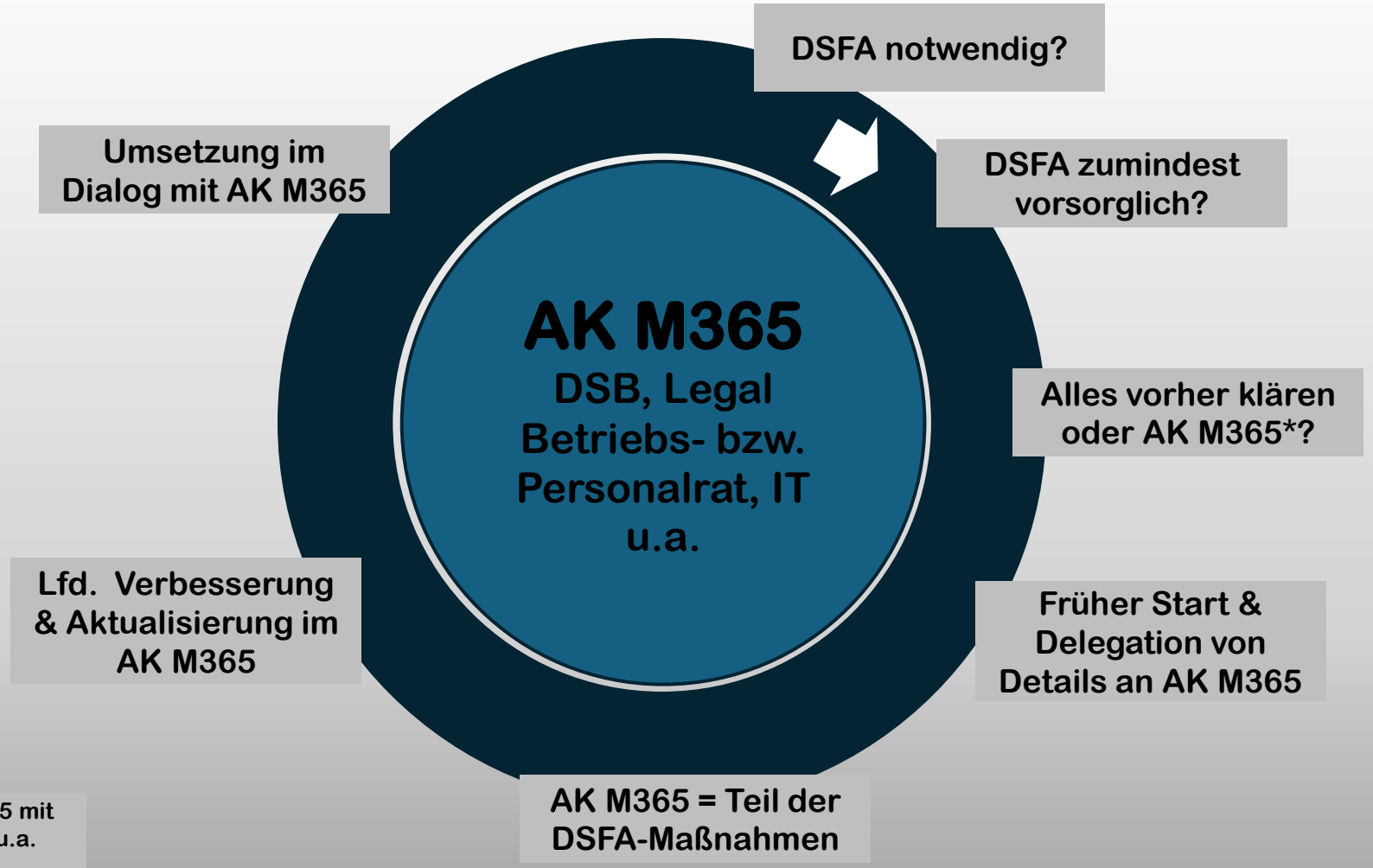
Hat die DSFA parat.

Datenschutz-Approval mit „agiler DSFA“ innerhalb von zwei Wochen.

LEGAL CHECK
www.legalcheck.digital

1

„Agile DSFA“ als Plan-Do-Check-Act
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

LEGAL CHECK
www.legalcheck.digital

2

2.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)

LEGAL CHECK
www.legalcheck.digital

3

3. Checkliste

Checkliste
DSFA M365

Inhalt: Checkliste für den Einsatz von Microsoft 365 zur Vorbereitung der rechtlichen Bewertung und der Erstellung der Datenschutz-Folgenabschätzung (DSFA) sowie weiterer Datenschutz-Dokumente	Checkliste: Stand 1/2025 Ausgefüllt am: Von:

1.	**Organisation / Anfragender**	
1.1	Voller rechtlicher Name Ihrer Organisation (exakte Firmierung / juristische Bezeichnung des Anfragenden oder für den Betrieb verantwortlichen (Bsp.: ACME Holding Services GmbH & Co. KG)	
1.2	Gebräuchliche Bezeichnung oder wesentliche Marke (Bsp.: BMW statt Bayerische Motoren Werke AG)	
1.3	Rechtliche Einordnung Ihrer Organisation: Unternehmen/Behörde/Universität/Gericht u.ä.; Verein/Stiftung/NGO/gGmbH u.ä.; Freiberufler; Kirchengemeinde i.S.d. Art. 91 DSGVO, Sonstige	
1.4	Wir gelten datenschutzrechtlich als a) private Stelle b) öffentliche Stelle c) Kirche etc. i.S.d. Art. 91 DSGVO d) DSGVO nicht anwendbar (Strafverfolgung, EU, ...) e) Unklar / weiß nicht	
1.5	Unsere (primäre) Datenschutz-Aufsichtsbehörde ist:	
1.6	Wir unterliegen besonderer Regulierung und/oder haben besonders sensible Daten (bitte beschreiben)	
4.5	Ergeben sich aus der Natur des Verantwortlichen (z.B. als öffentliche Stelle oder als Kirche iSd Art. 91 DSGVO) besondere Einschränkungen (z.B. zum „berechtigten Interesse“ durch Art. 6 Abs. 1 S. 2 DSGVO)?	
4.6	Ergeben sich aus der Natur der Daten (z.B. Art. 8, 9 oder 10 DSGVO) und/oder besonderer Regulierung besondere Einschränkungen (über die in Ziff. 4.3 genannten Umstände z.B. auch durch berufs- oder beamtenrechtliche Sondernormen)?	
5.	**IT-Landschaft, Lizenzen und Informationssicherheit / TOMs**	
5.1	Neben M365 werden i.d.R. auch weiterhin andere IT-Systeme genutzt werden, z.B. für HR oder CRM (auch Fachanwendungen genannt). Besteht ein Konzept, wo solche anderen Systeme „führendes System“ sind, also personenbezogene Daten primär dort verarbeitet werden, so dass die diesbezüglichen Daten nicht oder nur sporadisch in M365 verarbeitet werden? ➔ Siehe hierzu die Tabelle zu Ziff. 6.	
5.2	Welche M365-Lizenzen planen Sie zu nutzen bzw. verwenden Sie bereits (z.B. E3/E5)?	
5.3	Wie werden Sie Ihre Lizenzen (Pläne) beziehen?	

v3 © LegalCheck 2023-2025 www.legalcheck.digital

LEGAL CHECK
www.legalcheck.digital

5

Bsp. für einfache Maßnahmen (1/2): CIS-Benchmarks als Start für TOMs

Beispiel: Verwendung der kostenlosen CIS-Benchmarks für Einstellungen (TOMs) in M365-Admin-Centern.
Dazu Kap. 6.5, 6.6 der LegalCheck-Dokumente.

© CIS www.cisecurity.org/benchmark/microsoft_365

8.3 Teams devices **358**
8.4 Teams apps **358**
8.4.1 (L1) Ensure app permission policies are configured (Manual) 359
8.5 Meetings **361**
8.5.1 (L2) Ensure anonymous users can't join a meeting (Automated) 362
8.5.2 (L1) Ensure anonymous users and dial-in callers can't start a meeting (Automated) ... 365
8.5.3 (L1) Ensure only people in my org can bypass the lobby (Automated) 368
8.5.4 (L1) Ensure users dialing in can't bypass the lobby (Automated) 370
8.5.5 (L2) Ensure meeting chat does not allow anonymous users (Automated) 372
8.5.6 (L2) Ensure only organizers and co-organizers can present (Automated) 374
8.5.7 (L1) Ensure external participants can't give or request control (Automated) 376
8.5.8 (L2) Ensure external meeting chat is off (Automated) 379
8.5.9 (L2) Ensure meeting recording is off by default (Automated) 381
8.6 Messaging **383**
8.6.1 (L1) Ensure users can report security concerns in Teams (Automated) 384

8.5.1 (L2) Ensure anonymous users can't join a meeting (Automated)

Profile Applicability:

- E3 Level 2

Description:

This policy setting can prevent anyone other than invited attendees (people directly invited by the organizer, or to whom an invitation was forwarded) from bypassing the lobby and entering the meeting.

For more information on how to setup a sensitive meeting, please visit **Configure Teams meetings with protection for sensitive data - Microsoft Teams:** https://learn.microsoft.com/en-us/MicrosoftTeams/configure-meetings-sensitive-protection

Rationale:

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times.

Note: Those companies that don't normally operate at a Level 2 environment, but do deal with sensitive information, may want to consider this policy setting.

Impact:

Individuals who were not sent or forwarded a meeting invite will not be able to join the meeting automatically.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`
4. Under meeting join & lobby set `Anonymous users can join a meeting` to `Off`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting $false
```

Default Value:

On (True)

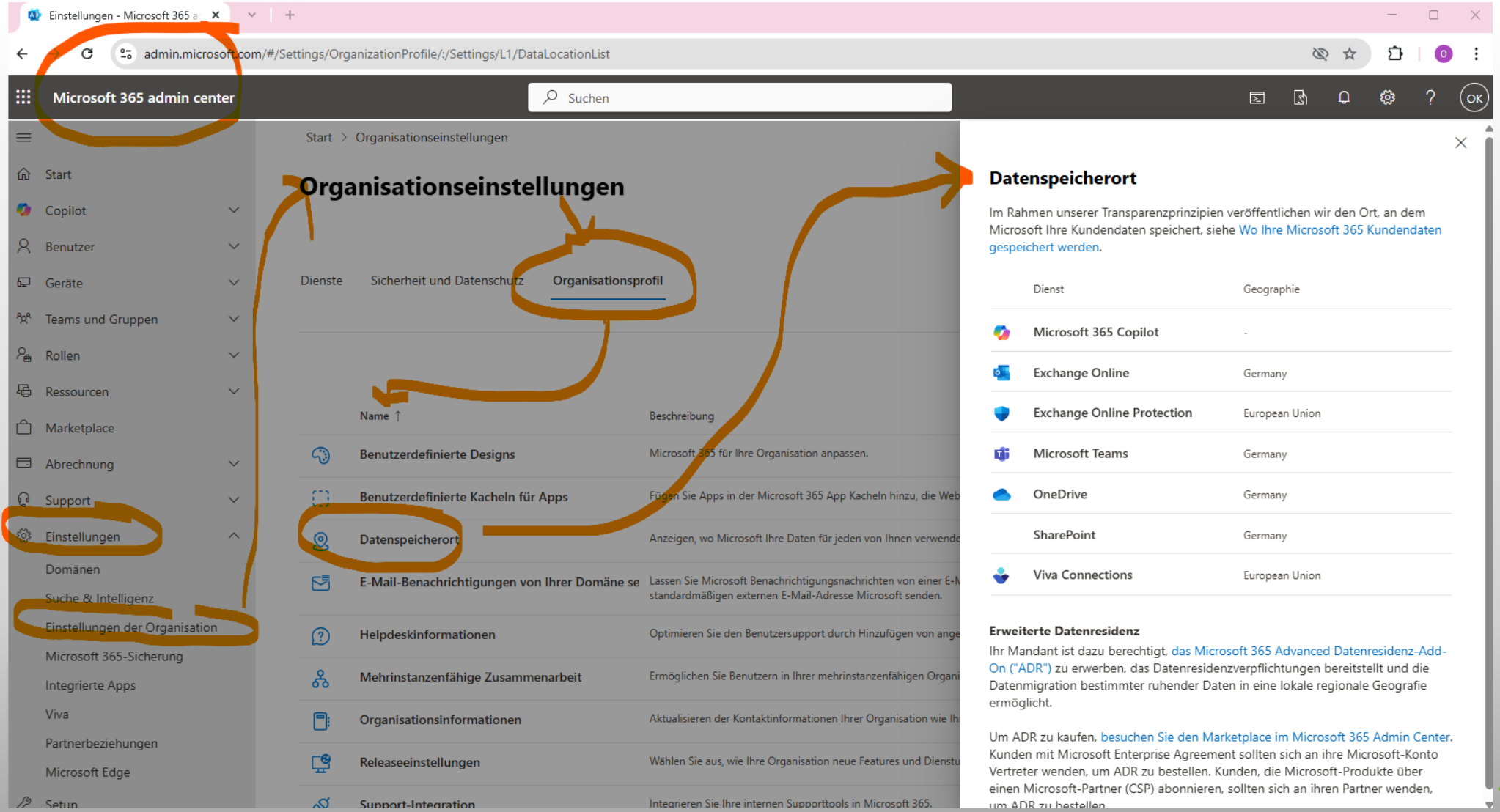
References:

1. https://learn.microsoft.com/en-us/MicrosoftTeams/configure-meetings-sensitive-protection

LEGAL CHECK
www.legalcheck.digital

5

Bsp. für einfache Maßnahmen (2/2): Check der „Datenspeicherorte“



LEGAL CHECK
www.legalcheck.digital

6

6. Risikomatrix von LegalCheck

xls zur Risikobewertung und -darstellung für die

Ursprungs- und Urheberrechtsvermerk
xls basierend auf "Risikomanagement-Tool – Vorlage" des Bundesverwaltungsamtes*
Bearbeitet von P.R., Dr. Olaf Koglin und LegalCheck
Version: 4/2025
© für diese Version/Bearbeitung: Olaf Koglin & LegalCheck 365 GmbH, Berlin
Nur zur internen Verwendung bei LegalCheck-Kunden

Disclaimer:
Die Verwendung dieses Dokuments erfolgt in eigener Verantwortung.
Der/die Verantwortlich(en) und etwaige Auftragsverarbeiter sind für die individuelle und zutreffende Aufnahme,

Risikoliste

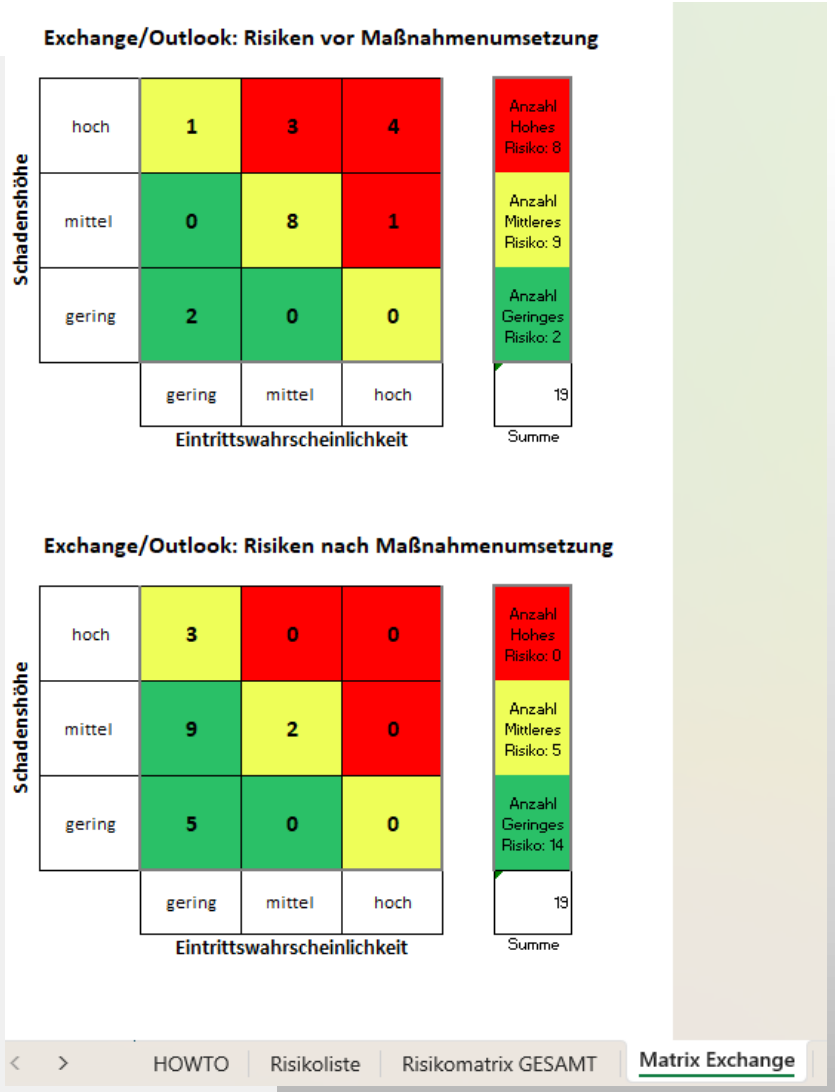
Risiko						Aktivitäten						Bereiche					Exchange / Outlook		Office		One
Nr.	Risikobeschreibung	EW	SA	Risiko	Risikofeld	Gegenmaßnahme	EW	SA	Risiko	Risikofeld	Übergeord. Exchange / Out.		Office	One Drive / Sharep.	Teams	Vor Maßnahm.	Nach Maßnahm.	Vor Maßnahm.	Nach Maßnahm.	Maßn.
100	**Allgemeine und rechtliche Risiken**																			
101	Vertrags- und Datenschutzsituation unklar, Verstoß gegen Rechtm.- und Rechenschaftspflicht	hoch	mittel	hoch	8	Recht. Prüfung Vertrag und insb. DPA (AVV etc.)	mittel	mittel	mittel	5	x	x	x	x	x	8	5	8	5	
102	Keine Dokumentation der Abschlusse von DPA und Zusatzvereinbarung, Verstoß Rechenschaftspflicht	mittel	mittel	mittel	5	Tatsächlicher Abschluss der DPA nebst Dokumentation, auch der Versionsnr.	gering	gering	gering	1	x	x	x	x	x	5	1	5	1	
105	Rechtliche Änderungen nach Abschluss, dadurch nachträglich entstehender Verstoß	mittel	hoch	hoch	7	Laufende Überprüfung im Hinblick auf Änderungen der rechtl. oder technischen	gering	gering	gering	1	x	x	x	x	x	7	1	7	1	
106	Kein Prozess zur Erfassung und Bewertung von späteren Änderungen	mittel	mittel	mittel	5	Festlegung eines Prozesses und von Zuständigkeiten für a.g. lfd. Überprüfungen	gering	gering	gering	1	x	x	x	x	x	5	1	5	1	
110	Verstoß Regelungen zum Drittlandtransfer und ggf. TIA	hoch	hoch	hoch	9	Rechtslage prüfen, ggf. TIA	mittel	mittel	mittel	5	x	x	x	x	x	9	5	9	5	
200	**Spezifische Risiken der Kunden bzw. Verantwortlichen (Übergreifend für alle MS-Produkte)**																			
205		hoch	hoch	hoch	9		gering	hoch	mittel	4	x	x	x	x	x	9	4	9	4	
206		hoch	hoch	hoch	9		gering	hoch	mittel	4	x	x	x	x	x	9	4	9	4	
207		mittel	hoch	hoch	7		gering	hoch	mittel	4	x	x	x	x	x	7	4	7	4	
210	Probleme in Zusammenarbeit [Gremium]	gering	gering	gering	1	Laufende Abstimmung	gering	gering	gering	1	x	x	x	x	x	1	1	1	1	
211	Meinungsänderung Personalrat	gering	gering	gering	1	Laufende Abstimmung; Stakeholder Management	gering	gering	gering	1	x	x	x	x	x	1	1	1	1	
212	Fehlende Datenschutzinformationen an Beschäftigte und Gäste	mittel	mittel	mittel	5	Erstellung & ggf. Schulungskonzept; ggf. Netiquette	gering	mittel	gering	2	x	x	x	x	x	5	2	5	2	
300	**Spezifische Risiken der Kunden bzw. Verantwortlichen (für einzelne MS-**																			
400	**Technische Risiken "in M365"**																			
410	Keine oder zu niedrige TOMs in den Admin-Centern von M365	hoch	hoch	hoch	9	Technische und organisatorische Maßnahmen mind. CIS Level 1	gering	mittel	gering	2	x	x	x	x	x	9	2	9	2	

LEGAL CHECK
www.legalcheck.digital

6

6. Risikomatrix von LegalCheck





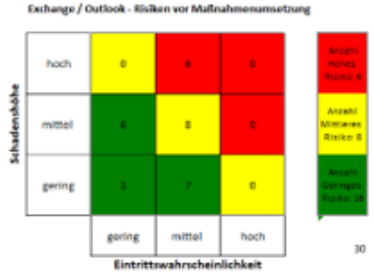
LEGAL CHECK
www.legalcheck.digital

7

7. Finalisierung DSFA-Dokument und …

Interesse im Sinne einer „IT-Straßenkriminalität" einschließlich der Erpressung zu „Ransom"-Zahlungen zu vermuten. Bei großen Rechenzentren wäre dies eher eine professionell-strategisch ausgerichtete Kriminalität, die sowohl von entsprechenden Kriminellen aus auch staatlichen, semi-staatlichen/politischen (wie Guerilla-Gruppen) oder NGO-artigen professionellen Kollektiven wie Anonymous ausgehen kann. Hinzuweisen ist dabei auch auf nach dem jeweiligen Landesrecht legale Auskunftsrechte von (Sicherheits-)Behörden. Insbesondere wenn sie sich primär gegen Daten von Ausländern richten oder in anderer Form als übergriffig erscheinen, werden sie im Ausland meist nicht geschätzt (wie aus europäischer Sicht gegenüber den USA der **CLOUD ACT** oder „FISA 702"; siehe hierzu Kap. 9.6.2.1 (S. 153).

Aus dieser Datenschutz-Folgenabschätzung und auf Basis festgestellten konkreten Situation des Verantwortlichen sowie den zur Begegnung der bislang festgestellten Risiken (siehe *Verwendete Dienste und zur Risikobegegnung* vorgesehene Maßnahmen, S. 108) ergeben sich **vor Maßnahmenumsetzung** folgende Risiken:



Risiken vor Maßnahmenumsetzung (Beispiel)

7.3.3.2 Word/PowerPoint/Excel Online

aa. Bewertung der Notwendigkeit und Verhältnismäßigkeit (konkret der Nutzung als SaaS):

i. Allgemein: Hier handelt es sich – anders als bei E-Mail ähnlicher Kommunikation – um Dokumente, die von den Mitarbeitern subjektiv als „eigene" Dateien angesehen werden. Die Mitarbeiter können Daten u.a. per Link sharen, also Dritten Zugriffsrechte geben, was über die Dokumenten-Speicherorte (OneDrive bzw. Sharepoint Online) abgebildet wird, also keine direkte Funktion von Word etc. ist.

ii. Konkret: Datenschutzrechtlich erscheint das Ersetzen von vollen Applikationen für Word, Powerpoint & Co. durch Software as a Service weitgehend unbedenklich. Zwar sind die Einstellungen für sog. Metadaten u.ä. sorgfältig zu beachten. Jedoch liegt der Schwerpunkt datenschutzrechtlicher Bedenken im Abspeichern der Dokumente sowie in der inhaltlichen Verarbeitung von Daten, d.h. in der Frage, welche (ggf. sensiblen) Informationen in den Dokumenten gespeichert werden. Dies ist bei Microsoft 365 jedoch grundsächlich nicht anders zu bewerten als bei installierten Applikationen.

8 KAPITEL 8: ENTSCHEIDUNG UND RAT DES DATENSCHUTZBEAUFTRAGTEN

Zusammenfassung durch den Verantwortlichen:

Der Einsatz von M365 beim Verantwortlichen bringt gewisse Risiken Betroffener mit sich, von denen viele jedoch in ähnlichem Maße auch bei einer on-premise Lösung eintreten.

Hiergegen werden die hier und in anderen Dokumenten beschriebenen und noch weiter zu konkretisierenden Abhilfemaßnahmen geplant, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren. Durch diese wird der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird (Art. 35 Abs. 7 lit. (d) DSGVO).

8.1 Rat des Datenschutzbeauftragten im Rahmen der DSFA

Die/Der Datenschutzbeauftragte hat die vorgelegte DSFA erhalten. Sein Rat lautet:

☐ Der geplante Einsatz von Microsoft 365 kann mit den oben beschriebenen Produkten ohne weitere Maßnahmen oder Einschränkungen durchgeführt werden.

☐ Für den geplanten Einsatz von Microsoft 365 mit den oben beschriebenen Produkten wird empfohlen, Maßnahmen für die Reduzierung der Risiken der Betroffenen vorzunehmen, nämlich:

- ☐ eine oder mehrere der oben unter Kap. 7.3.5 (S. 133) beschriebenen Abhilfemaßnahmen
  und/oder
- ☐ folgende konkrete Maßnahme(n):
  (ggf. separat aufführen)

_____

_____

_____
Datum, Name, Unterschrift der/des Datenschutzbeauftragten

8.2 Entscheidung des Verantwortlichen (durch die Geschäftsführung)

Der Verantwortliche hat gem. Art. 35 Abs. 2 DSGVO den Rat des Datenschutzbeauftragten eingeholt. Seine Hinweise sind vor Beginn der Verarbeitung angemessen zu berücksichtigen. Sodann kann, unter Berücksichtigung aller anderen Voraussetzungen, mit dem Einsatz von Microsoft 365 im beschriebenen Umfang begonnen werden.

Hinweis: Sofern aus der DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, ist gem. Art. 36 Abs. 1 DSGVO eine sog. Vorherige Konsultation bei der Datenschutz-Aufsichtsbehörde durchzuführen, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

_____ _____

Datum, Name, Unterschrift Datum,

Name, Unterschrift

Kundenname

LEGAL CHECK
www.legalcheck.digital

8

8. 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

LEGAL CHECK
www.legalcheck.digital

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.

- ✓ 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



Dr. Olaf Koglin
Rechtsanwalt,
Geschäftsführer LegalCheck

Sie haben noch Fragen?
Wir unterstützen Sie gerne.

ok@legalcheck.digital | www.legalcheck.digital