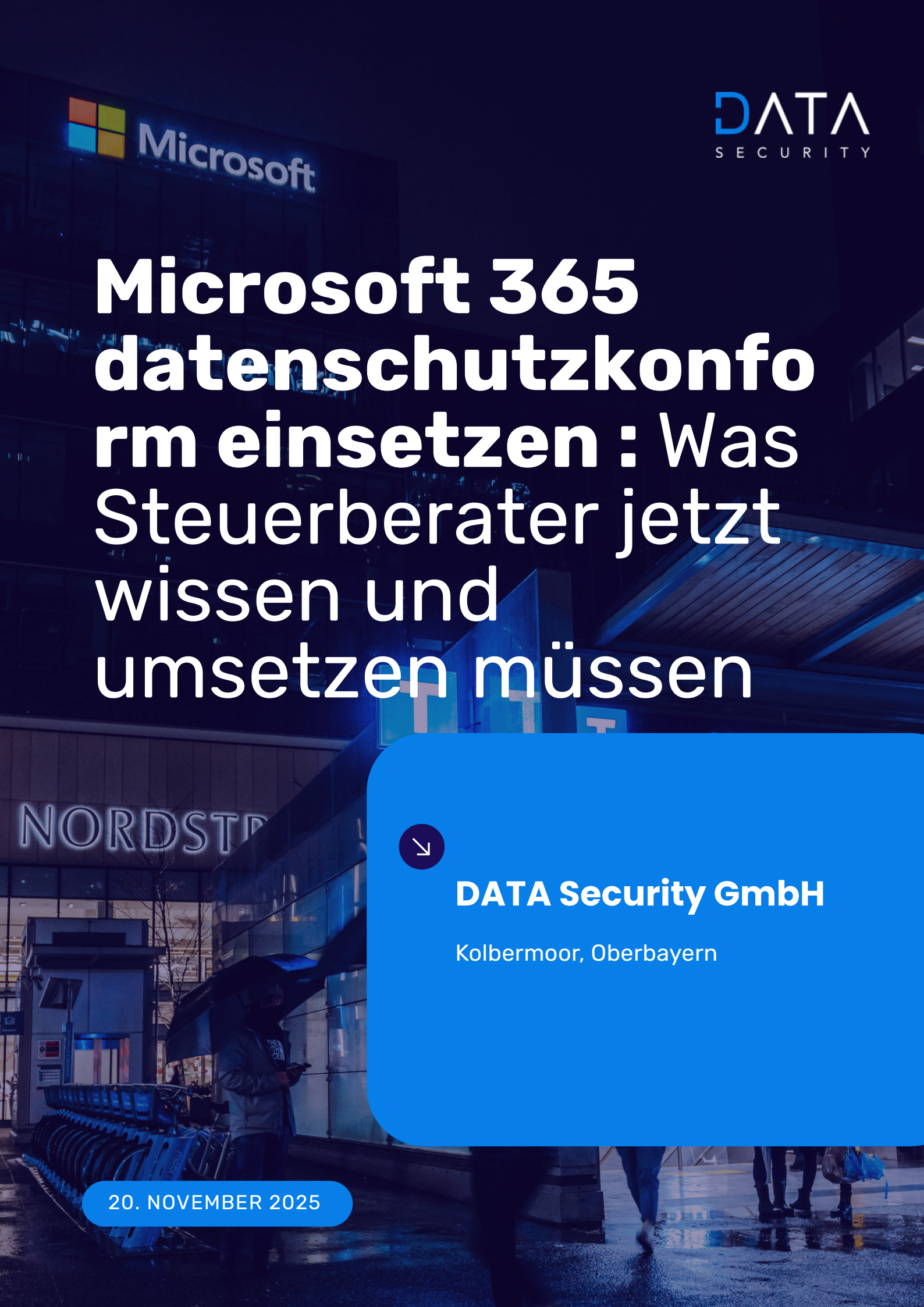


DATA SECURITY

Microsoft 365 datenschutzkonform einsetzen: Was Steuerberater jetzt wissen und umsetzen müssen

DATA Security GmbH

Kolbermoor, Oberbayern

20. NOVEMBER 2025

Management Summary

Dieses Whitepaper zeigt Steuerkanzleien, wie sie Microsoft 365 sicher und datenschutzkonform einsetzen können – praxisorientiert und effizient. Im Fokus stehen konkrete Maßnahmen, technische Einstellungen und organisatorische Schritte, die notwendig sind, um die Anforderungen der DSGVO, des BDSG und der Aufsichtsbehörden zu erfüllen.

Zielgruppe: Steuerberater, IT-Verantwortliche und Datenschutzbeauftragte in Kanzleien.
Nutzen: Orientierung, Umsetzungshilfe und Nachweisführung im Rahmen der Rechenschaftspflicht.

Kapitel 1 – Der rechtliche Rahmen: DSGVO, BDSG und Auftragsverarbeitung

Wer Microsoft 365 in der Steuerberatung einsetzt, agiert rechtlich gesehen als Verantwortlicher nach Art. 4 Nr. 7 DSGVO. Das bedeutet: Die Kanzlei entscheidet über Zweck und Mittel der Verarbeitung personenbezogener Daten – und trägt somit die Hauptverantwortung.

Der Einsatz von Microsoft 365 entbindet die Kanzlei nicht von ihren Pflichten. Auch wenn Microsoft hier im Regelfall als Auftragsverarbeiter agiert, bleibt die Kanzlei verpflichtet, die Datenverarbeitung zu überwachen, die vertraglichen Regelungen zu prüfen und geeignete technische sowie organisatorische Maßnahmen umzusetzen.

Wichtige Grundlagen

- Art. 28 DSGVO – Auftragsverarbeitung: AVV mit Microsoft erforderlich; Prüfung der Online Service Terms (OST) und Data Protection Addendum (DPA).
- Art. 5 DSGVO – Grundsätze der Verarbeitung: Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Integrität.
- Art. 32 DSGVO – Sicherheit der Verarbeitung: MFA, Verschlüsselung, DLP, Zero Trust und Logging müssen konfiguriert werden.
- Internationale Datentransfers: Prüfung des EU-US Data Privacy Framework und Dokumentation der Datenflüsse.
- Kurz gesagt: DSGVO-Compliance ist keine Checkbox, sondern eine Daueraufgabe – und wer seine Verantwortung auf Microsoft abschiebt, riskiert Ärger mit der Aufsichtsbehörde.

Kapitel 2 – Risikoanalyse und Datenschutzfolgeabschätzung

Eine regelmäßige und nachvollziehbare Risikoanalyse ist das Fundament jeder datenschutzkonformen Nutzung von Microsoft 365. Sie bewertet, welche Gefahren für die Rechte und Freiheiten betroffener Personen bestehen, und dient als Bewertungsgrundlage, ob eine Datenschutzfolgeabschätzung (DSFA) erforderlich ist.

Empfohlenes Vorgehen:

1. Systematische Erfassung aller Microsoft-365-Dienste, die personenbezogene Daten verarbeiten.

2. Bewertung der Eintrittswahrscheinlichkeit und Schwere möglicher Risiken.

3. Ableitung technischer und organisatorischer Maßnahmen.

4. Dokumentation der Ergebnisse für den Nachweis gegenüber der Aufsichtsbehörde.

Tipp: Als zusätzliches Werkzeug zur Bewertung und Dokumentation von Datenschutz- und Sicherheitsrisiken kann Sie der Microsoft Compliance Manager unterstützen. Dieser ersetzt jedoch keine eigenständige Risikoanalyse oder DSFA.

DATA SECURITY

Kapitel 3 – Der Microsoft 365 Tenant: Struktur, Identitäten und Verantwortung

Der Tenant bildet die logische Organisationseinheit innerhalb von Microsoft 365.

Er trennt die Daten eines Vertragspartners (z. B. einer Kanzlei oder eines Unternehmens) von anderen Mandanten in der Microsoft-Cloud und definiert damit den organisatorischen Rahmen der Datenverarbeitung.

Durch die Zuweisung von Lizenzen und Diensten innerhalb des Tenants (z. B. Exchange Online, Teams, SharePoint) wird festgelegt, welche Datenverarbeitungen tatsächlich stattfinden und welche Funktionen verfügbar sind.

Eine klare und strukturierte Tenant-Architektur ist daher eine wesentliche Voraussetzung für Sicherheit, Datenschutz und Nachvollziehbarkeit.

Wichtige Aspekte:
Trennung produktiver und testweiser Umgebungen zur Minimierung unbeabsichtigter Datenverarbeitung.

Klare Vergabe von Rollen und Berechtigungen nach dem Prinzip der minimalen Rechte (Least Privilege).

Regelmäßige Überprüfung inaktiver Konten und externer Gastzugänge.
Dokumentation administrativer Verantwortlichkeiten und Protokollierung von Änderungen.

Hinweis:
Die Verantwortung für dessen korrekte Einrichtung und Verwaltung liegt beim Verantwortlichen nach Art. 4 Nr. 7 DSGVO – also bei der Kanzlei bzw. dem Unternehmen.

Kapitel 4 – Microsoft 365 Lizenzierung und Datenschutzfunktionen

Die Wahl der richtigen Lizenz ist entscheidend für den Umsetzung von Datenschutz- und Sicherheitsanforderungen.

Viele Sicherheits- und Compliance-Funktionen stehen nur in den höheren Lizenzmodellen (z. B. Microsoft 365 E5 oder Business Premium) zur Verfügung.

Wichtige Lizenzunterschiede

- Business Standard: Basisfunktionen ohne DLP, ohne Compliance Center, eingeschränkte Security Tools.
- Business Premium: Enthält Microsoft Defender, Intune, Azure AD Premium P1 – ideal für kleinere Kanzleien.
- Microsoft 365 E3: Erweiterte Sicherheits- und Compliance-Funktionen, ohne erweiterte Analysen.
- Microsoft 365 E5: Vollständiges Sicherheits- und Compliance-Paket inkl. DLP, Insider Risk Management, Audit Logs, eDiscovery, und Purview.

Empfehlung: Aus Datenschutz- und Compliance-Sicht empfiehlt es sich mindestens Microsoft 365 Business Premium, besser noch E3 oder E5 einzusetzen, um Datenschutzanforderungen richtig konfigurieren, dokumentieren und regelmäßig überwachen zu können.

Kapitel 5 – Sicherheitseinstellungen in Microsoft 365

Eine datenschutzkonforme Konfiguration von Microsoft 365 setzt eine hohe Informationssicherheit voraus.

Microsoft 365 bietet zahlreiche Funktionen, um Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten – diese müssen jedoch bewusst aktiviert, regelmäßig überprüft und gepflegt werden.

Zentrale Maßnahmen

- Multifaktor-Authentifizierung (MFA) für alle Benutzer – Pflicht für jede Kanzlei.
- Bedingter Zugriff zur Kontrolle von Anmeldebedingungen.
- Geräteverwaltung über Intune und Richtlinien für mobile Endgeräte.
- Datenverschlüsselung (BitLocker, TLS, E-Mail-Verschlüsselung).
- Schutz sensibler Informationen mit Microsoft Purview.
- Überwachung durch Audit-Logs im Microsoft 365 Defender.

Sicherheit ist kein Zustand, sondern ein fortlaufender Prozess. Kanzleien sollten ihre Microsoft-365-Umgebung regelmäßig überprüfen und die Sicherheitsbewertung (Secure Score) im Microsoft-365-Defender nutzen, um die Wirksamkeit ihrer Schutzmaßnahmen zu verbessern.

Kapitel 6 – Sicherheits- und Compliance-Management

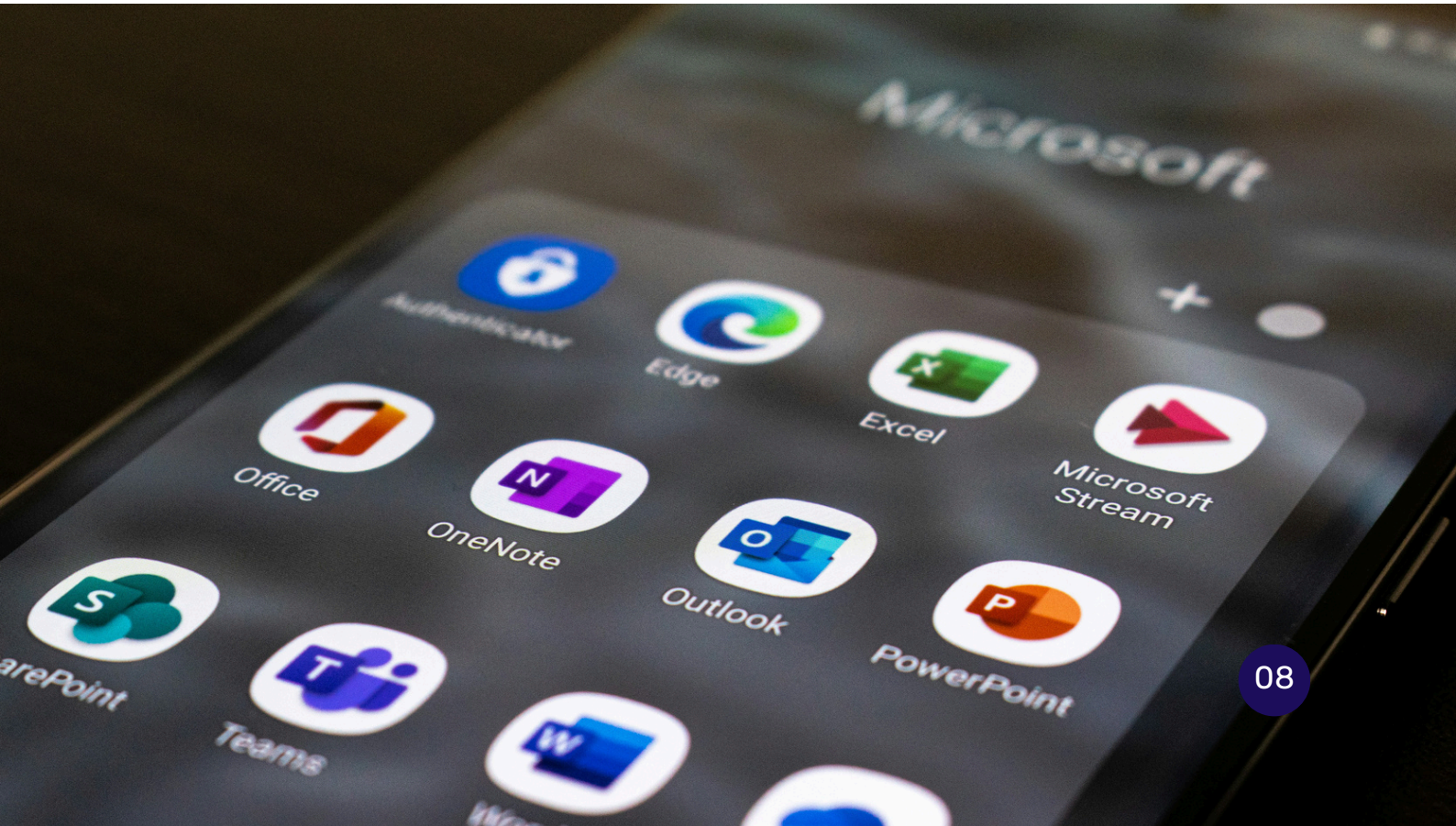
Ein zentrales Element des Datenschutzes ist ein fortlaufendes Sicherheits- und Compliance-Management. Microsoft 365 stellt mit dem Microsoft Purview Compliance-Portal hierfür leistungsstarke Werkzeuge bereit, um Richtlinien zu erstellen, deren Einhaltung zu überwachen, Verstöße zu erkennen und Nachweise zu dokumentieren.

Best Practices für Steuerkanzleien

Nutzung des Compliance Managers zur Bewertung des Umsetzungsstands der DSGVO-Anforderungen und technischer Sicherheitsmaßnahmen.

- Überwachung von Aktivitäten durch Audit-Logs und Alerts.
- Implementierung von Aufbewahrungsrichtlinien für steuerrelevante Dokumente.
- Schulung der Mitarbeiter zu Datenschutz- und Sicherheitsanforderungen.

Durch den gezielten Einsatz dieser Werkzeuge kann die Kanzlei die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nachweisbar unterstützen und zugleich Sicherheitsrisiken deutlich reduzieren.



DATA SECURITY

Kapitel 7 – Zugriff durch Behörden & internationale Datenübertragungen

Ein zentraler Kritikpunkt beim Einsatz von Microsoft 365 ist die **rechtliche Möglichkeit eines Datenzugriffs oder einer Sperrung des Zugriffs durch US-amerikanische Behörden** auf personenbezogene Daten.

Grundlage hierfür ist **unter anderem der US CLOUD Act**, der US-Unternehmen wie Microsoft unter bestimmten Voraussetzungen zur **Herausgabe oder Offenlegung von Daten verpflichtet – auch dann, wenn diese in europäischen Rechenzentren gespeichert sind.**

Seit Inkrafttreten des **EU-US Data Privacy Frameworks (DPF)** im Jahr 2023 besteht ein neuer **Angemessenheitsbeschluss der EU-Kommission**, der Datenübermittlungen in die USA erleichtert.

Der Beschluss stützt sich maßgeblich auf die **Executive Order 14086** („Enhancing Safeguards for U.S. Signals Intelligence Activities“) sowie auf ergänzende **US-Justizvorschriften**, durch die unter anderem das **Data Protection Review Court (DPRC)** geschaffen wurde.

Diese Regelungen sind exekutivrechtlicher Natur und können durch die US-Regierung angepasst werden. Sie schaffen zwar einen formalen Rechtsrahmen, ersetzen jedoch nicht die Pflicht der Verantwortlichen, Datenflüsse und Zugriffsrisiken eigenständig zu bewerten und zu dokumentieren.

Seit Inkrafttreten des EU-US Data Privacy Frameworks (DPF) im Jahr 2023 besteht ein neuer Angemessenheitsbeschluss der EU-Kommission, der Datenübermittlungen in die USA erleichtert.

DATA SECURITY

Der Beschluss stützt sich maßgeblich auf die **Executive Order 14086** („Enhancing Safeguards for U.S. Signals Intelligence Activities“) sowie auf ergänzende **US-Justizvorschriften**, durch die unter anderem das **Data Protection Review Court (DPRC)** geschaffen wurde.

Diese Regelungen sind exekutivrechtlicher Natur und können durch die US-Regierung angepasst werden. Sie schaffen zwar einen formalen Rechtsrahmen, ersetzen jedoch nicht die Pflicht der Verantwortlichen, Datenflüsse und Zugriffsrisiken eigenständig zu bewerten und zu dokumentieren.

Empfohlene Maßnahmen:

Dokumentation aller Microsoft-Dienste, die personenbezogene Daten verarbeiten oder speichern.

Überprüfung der Vertragsunterlagen (Online Service Terms, Data Protection Addendum) auf aktuelle datenschutzrechtliche Anforderungen.

Bewertung der Zugriffsmöglichkeiten über Funktionen wie Customer Lockbox und Advanced Audit.

Hinweis:
Kanzleien sollten ihren Mandanten gegenüber **transparent kommunizieren**, wie Daten geschützt werden, welche Sicherheitsvorkehrungen zum Einsatz kommen und welche Verantwortlichkeiten zwischen Kanzlei und Microsoft bestehen.

Kapitel 8 – Umsetzung in der Kanzlei: Von der Theorie zur Praxis

Datenschutz in Microsoft 365 entsteht nicht allein durch technische Einstellungen – er lebt von klaren Prozessen, bewusster Verantwortung und regelmäßigen Schulungen.

Dieses Kapitel beschreibt, wie Kanzleien die Einführung von Microsoft 365 strukturiert planen, umsetzen und fortlaufend verbessern können - von der Festlegung der Verantwortlichkeiten bis zur regelmäßigen Überprüfung der Wirksamkeit.

Praktische Schritte

1. Verantwortlichkeiten definieren: Datenschutzbeauftragter, IT-Administrator, Fachverantwortliche.

2. Berechtigungskonzept erstellen: Wer darf welche Daten sehen, bearbeiten, teilen?

3. Richtlinien für Dateiablage und Teams-Struktur festlegen: eindeutige Ablagestrukturen und klare Benennungsregeln

4. Regelmäßige Datenschutz- und IT-Sicherheits-Schulungen durchführen: Mitarbeitende sensibilisieren

5. Audit-Trails und Berichte regelmäßig prüfen und dokumentieren: als Nachweise gegenüber Aufsichtsbehörden.

Hinweis: Einmalige Maßnahmen reichen nicht - Datenschutz und Informationssicherheit sind laufende Prozesse der kontinuierlichen Verbesserung.

Kapitel 9 – Checkliste & Maßnahmenplan

Praxisorientierte Checkliste für Steuerkanzleien

Zur Unterstützung finden Sie hier eine praxisorientierte Checkliste mit den wichtigsten Aufgaben für eine datenschutzkonforme **Nutzung von Microsoft 365 in Steuerkanzleien:**

✅ Abschluss und Prüfung des Auftragsverarbeitungsvertrags (AVV) mit Microsoft dokumentieren
✅ Tenant-Struktur analysieren und Rollen- sowie Berechtigungen regelmäßig prüfen
✅ Multifaktor-Authentifizierung (MFA) für alle Benutzer aktivieren
✅ Data Loss Prevention (DLP) und Sensitivity Labels konfigurieren
✅ Zugriffsrechte und Freigaben regelmäßig prüfen
✅ Datentransfers in Drittländer dokumentieren (z. B. im Verzeichnis der Verarbeitungstätigkeiten)
✅ Mitarbeitende regelmäßig schulen und Datenschutz-Awareness fördern
✅ Audit-Logs aktivieren und regelmäßig auswerten zur Nachvollziehbarkeit von Aktivitäten
✅ Notfallkonzept für Datenschutzverletzungen definieren und Meldeprozesse dokumentieren
✅ Jährliche Überprüfung der Datenschutz- und Sicherheitsmaßnahmen durchführen

Hinweis:
Die regelmäßige Umsetzung dieser Maßnahmen sollte Bestandteil des jährlichen Datenschutz- und IT-Sicherheitsaudits der Kanzlei sein.

Kapitel 10 – Ausblick & Weiterentwicklung

Microsoft 365 und die Datenschutzanforderungen entwickeln sich stetig weiter.

Neue Funktionen wie **KI-gestützte Analysen**, **Copilot** und **automatisierte Klassifizierungen** erweitern nicht nur die Möglichkeiten der Zusammenarbeit, sondern bringen zugleich **neue Herausforderungen für Datenschutz**, **Informationssicherheit und Compliance** mit sich.

Kanzleien sollten daher ihre **Datenschutzstrategie**, **Prozesse und Richtlinien regelmäßig überprüfen**, neue Funktionen **kritisch bewerten** und bei Bedarf **anpassen**.

Eine enge Zusammenarbeit zwischen **IT, Datenschutzbeauftragtem und Geschäftsführung** bleibt der Schlüssel zu einer dauerhaft **sicheren und rechtskonformen Nutzung**.

Fazit:
Microsoft 365 ist kein Risiko, wenn es **bewusst, kontrolliert und transparent eingesetzt** wird.

Mit klaren Prozessen, den richtigen Einstellungen und einem wachsamen Blick auf neue Entwicklungen lassen sich **Datenschutz und Digitalisierung erfolgreich vereinen**.

Editorial

Die Autoren

Salomo Dobberschütz ist Microsoft 365 Compliance Berater bei der DATA Security GmbH und unterstützt Unternehmen bei der sicheren und regelkonformen Nutzung ihrer Microsoft-Cloud-Umgebungen. Als erfahrener Spezialist für Microsoft 365, Azure (Entra) und moderne Sicherheitsarchitekturen verbindet er technische Tiefe mit praxisnaher Compliance-Beratung.

Seine berufliche Erfahrung umfasst Tätigkeiten als Cloud Service & Lizenzberater für Microsoft, VMware (Broadcom), Veeam und Citrix sowie als IT-Cloud Engineer. Zudem war er im Microsoft-Helpdesk im 1st- und 2nd-Level-Support tätig, arbeitete als IT-System-Security Manager, Azure-(Entra-) und Netzwerkadministrator, MDM-Spezialist sowie als Administrator für SharePoint Online und Exchange Online. Weitere Expertise bringt er aus seiner Arbeit als Microsoft Dynamics CRM Consultant und als Datenschutzspezialist im Bildungsbereich mit.

Als Microsoft 365 Certified – Enterprise Administrator Associate sowie zertifizierter Datenschutzberater, Geldwäsche-Compliance-Beauftragter und KI-Compliance-Berater (gemäß EU-KI-Verordnung) konzentriert er sich heute auf die pragmatische Umsetzung regulatorischer Anforderungen in Microsoft-365- und Azure-Umgebungen. Sein Fokus liegt auf technischen und organisatorischen Lösungen, die Compliance sicherstellen, ohne unnötigen Mehraufwand zu erzeugen, und Unternehmen optimal auf Prüfungen vorbereiten.

Milomir Mikulovic ist Senior Berater bei der DATA Security GmbH und unterstützt Steuerberater, Wirtschaftsprüfer, Rechtsanwälte und sonstige Mandanten bei der digitalen Transformation ihrer Compliance-Prozesse. Als zertifizierter Experte für Datenschutz (DSGVO), Geldwäscheprävention, Hinweisgeberschutz sowie ISO 9001/27001 hat er sich auf die pragmatische Umsetzung regulatorischer Anforderungen spezialisiert.

Sein Fokus liegt auf automatisierten Lösungen, die rechtssichere Dokumentation ohne manuellen Mehraufwand gewährleisten und Unternehmen auf behördliche Prüfungen optimal vorbereiten. Zusätzliche Schwerpunkte seiner Arbeit umfassen KI-Compliance (KI-VO) und die sichere Implementation von MS365-Umgebungen

Die DATA Security ermöglicht Organisationen im deutschsprachigen Raum, Datenschutz, Informationssicherheit und Compliance praxisorientiert und rechtskonform zu etablieren. Details zu unserem Leistungsspektrum finden Sie unter: www.data-security.one

Bei Fragen oder für einen fachlichen Austausch erreichen Sie die Autoren direkt über LinkedIn.
Disclaimer: Die hier präsentierten Ausführungen spiegeln die fachliche Einschätzung der Autoren wider. Für die Richtigkeit und Vollständigkeit der Inhalte wird keine Haftung übernommen. Eine individuelle Beratung im konkreten Einzelfall bleibt unerlässlich.

Kontakt

Büro:

Carl-Jordan-Str. 14
83059 Kolbermoor
Bayern, Deutschland

Telefon:

+49 (0)8031 2300 100

E-Mail :

info@data-security.one