PROVECTUS

Datenschutz und Compliance

mit Microsoft 365

INHALT

MICROSOFT 365 IN DER CLOUD // 03

RECHTLICHE GRUNDLAGEN: Verschärfte Gesetze für die IT-Sicherheit // 06

DIE DATENSCHUTZ-FOLGEABSCHÄTZUNG // 09

- **WANN** muss eine Datenschutz-Folgeabschätzung vorgenommen werden? // 11
- **WIE** läuft eine Datenschutz-Folgeabschätzung ab? // 12

MASSNAHMEN für den datenschutzkonformen Einsatz von Microsoft 365 // 16

HANDLUNGSEMPFEHLUNGEN für Datenschutz & Compliance in einer Evergreen IT // 21

MICROSOFT TEAMS // 24

- **DATENSCHUTZRISIKEN** mit Microsoft Teams // 25
- **DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN** // 27

FAZIT // 29

MICROSOFT 365 IN DER CLOUD

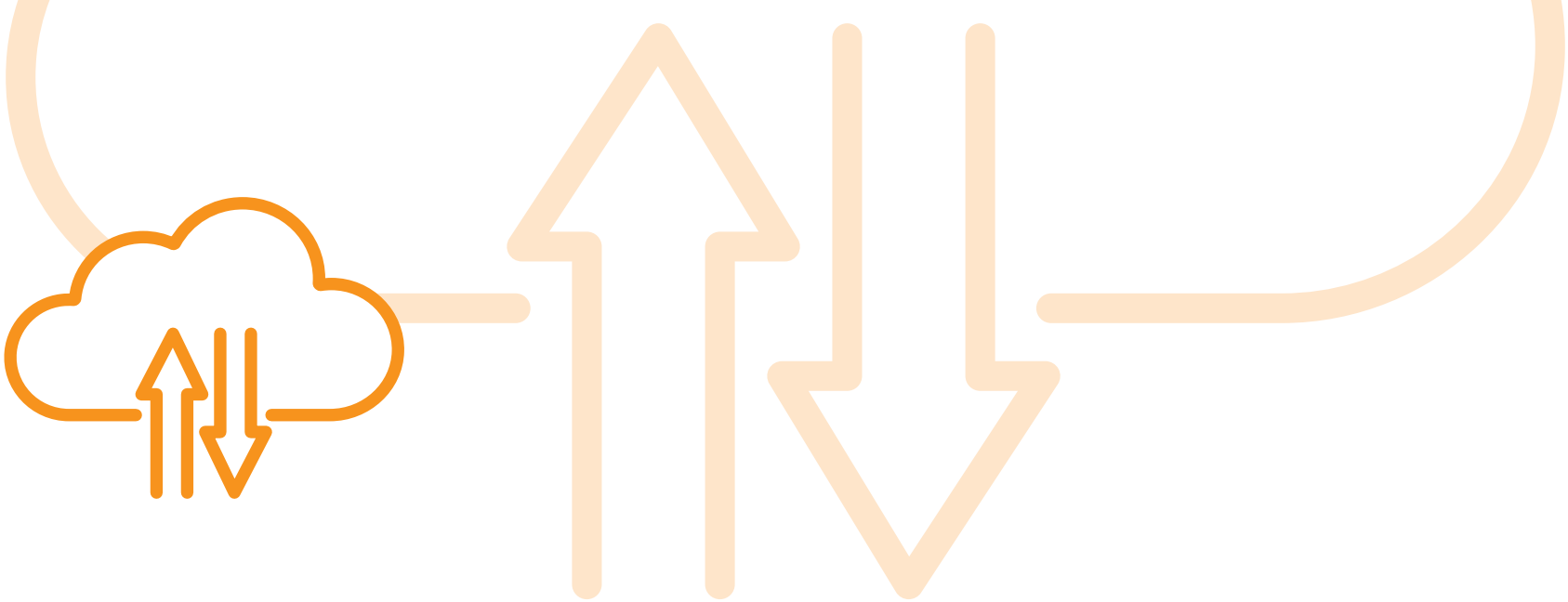
MICROSOFT 365 IN DER CLOUD

Compliance und Datenschutz sind in vielen Unternehmen ein sensibles Thema, denn wer personenbezogene Daten erhebt, speichert und verarbeitet, ist gesetzlich dazu verpflichtet sie bestmöglich zu schützen. Mit dem Umzug in die Microsoft Cloud haben Unternehmen die Möglichkeit, die eigenen Infrastruktur flexibel anzupassen und die Verwaltung ihrer IT zu vereinfachen. Doch die Nutzung der Microsoft Cloud bedeutet für sie zwangsläufig auch einen Kontrollverlust, denn ihre Daten befinden sich nicht mehr auf den eigenen Servern, sondern werden in Rechenzentren von Microsoft gespeichert. Diese orientieren sich zwar am europäischen Datenschutz, sind jedoch auf einen weltweiten Kundenkreis ausgerichtet. Deshalb gehen die Meinungen auseinander, wenn es darum geht, inwieweit Microsoft 365 hierzulande datenschutzkonform eingesetzt werden kann.

Microsoft Deutschland hat hierzu bereits in der Vergangenheit eine Stellungnahme herausgegeben. Dort heißt es, dass alle Microsoft-Produkte und -Dienste sowohl in der Privatwirtschaft als auch im öffentlichen Sektor unter Einhaltung aller Regelungen des Datenschutzes eingesetzt werden können (Quelle: Stellungnahme von Microsoft Deutschland zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams)

Auf den Vorwurf, dass ein Datentransfer in Drittstaaten wie die USA unzulässig ist, argumentiert Microsoft, dass die DSGVO eine Übermittlung in Drittstaaten, einschließlich der USA, dann rechtens ist, wenn diese unter Nutzung von geeigneten Garantien (z.B. Standardvertragsklauseln 2021/914 und zusätzlicher Maßnahmen) stattfindet. In diesem Zuge müssen Unternehmen jedoch dafür sorgen, eine Risikoanalyse im Lichte der Schrems–II-Rechtsprechung des EuGH durchzuführen und ggf. zusätzliche Maßnahmen implementieren.

Genau hier liegt die Krux an der Sache. Denn mit der Rechtsprechung des EuGH, die den Transfer personenbezogener Daten zwischen der EU und den USA durch



das Privacy Shield ohne Übergangsfristen für unwirksam erklärt hat, sind Unternehmen nun auf sich gestellt. Jede Firma muss die in der Stellungnahme angesprochenen Risikoanalysen und Schutzmaßnahmen selbst realisieren. Mit den vorgegebenen Datenschutzkonfigurationen ist Microsoft 365 hierzulande also datenschutzwidrig. Das bedeutet, dass Unternehmen, die Microsoft 365 in Betrieb haben, eigens tätig werden müssen, um den DSGVO-konformen Einsatz der Anwendungen gewährleisten zu können. Hierfür müssen sie ein ordnungsgemäßes IT-Risikomanagement zur Nutzung von Microsoft-365-Diensten nachweisen. Andernfalls drohen mögliche Bußgelder und Schadenersatzforderungen seitens der Behörden. Anders als im deutschen Zivilrecht können letztere nicht nur zum Ausgleich entstandener Nachteile gefordert werden, sondern auch zur Abschreckung, um weitere Verstöße unattraktiv zu machen, verhängt werden. Dabei sind Strafen von bis zu 20 Millionen oder 4 Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem welcher Wert höher ist, möglich.

Wir erklären, worauf es dabei ankommt, welche rechtlichen Grundlagen nicht außer Acht gelassen werden dürfen und geben wertvolle Handlungsempfehlungen für den datenschutzkonformen Einsatz von Microsoft Teams in ihrem Unternehmen.

RECHTLICHE GRUNDLAGEN

VERSCHÄRFUNG VON IT-SICHERHEIT

Die Bedrohungslage für IT-Infrastrukturen ist in den vergangenen Jahren exponentiell gestiegen. Spätestens seit dem Überfall auf die Ukraine wurde deutlich, dass auch im Cyberspace ein Krieg tobt. Doch auch schon lange vor Ausbruch des Krieges wurden gezielt Cyber-Angriffe durchgeführt. Ziel war dabei längst nicht mehr nur das Erbeuten von Geld, sondern auch das (Zer-)Stören und Ausspionieren.

Bereits im Sommer 2015 hat die Bundesregierung deshalb ein neues IT-Sicherheitsgesetz auf den Weg gebracht. Ein zweites Gesetz zur Erhöhung des Schutzes informationstechnischer Systeme trat im Mai 2021 in Kraft. Es sieht vor, dass Betreiber kritischer Infrastrukturen (KRITIS) Systeme zur Angriffserkennung im Einsatz haben müssen. Mit den gesteigerten Sicherheitsmaßnahmen will die Bundesregierung den Schutz von Unternehmen, Behörden und auch der Bevölkerung selbst gegenüber Cyberangriffen verstärken.

In Zukunft wird eine weitere Revision des IT-Sicherheitsgesetzes erwartet. Dieses soll die EU NIS-2-Richtlinie aufgreifen und weitere Anforderungen für KRITIS-Betreiber festlegen. Wann KRITIS 3.0 in Kraft tritt und was es genau beinhalten wird, bliebt allerdings bislang offen.

Was sind KRITIS Sektoren?

Der KRITIS-Sektor betrifft Bereiche, die für das Gemeinwesen von zentraler Bedeutung sind, bei deren Ausfall oder Beeinträchtigung wesentliche Versorgungsengpässe, Störungen der öffentlichen Sicherheit sowie weitere Folgen, welche die Öffentlichkeit nachhaltig beeinträchtigen, eintreten können. Dazu zählen Unternehmen aus den Bereichen Energie, Transport und Verkehr, Abwasser, Trinkwasser, Finanz- und Versicherungswesen, Gesundheit, Informations- und Telekommunikationstechnik, Verwaltung von Informations- und Kommunikations-Diensten (ITK) für Business-to-Business-Kunden oder Weltraum. Außerdem fallen bestimmte Arten von Logistik, Entsorgung, Produktion, Chemie, Ernährung und verarbeitendem Gewerbe, digitaler Dienste und Forschung unter das KRITIS-Dachgesetz.

Technische Pflichten und Anzeigepflichten

Nach §8b BSIG müssen sich Betreiber kritischer Infrastrukturen beim BSI und registrieren. Darüber hinaus sind sie verpflichtet, eine Kontaktstelle zu benennen, über die sie jederzeit erreichbar sind. Verweigert ein Unternehmen die Registrierung ist das BSI in Zukunft berechtigt, die Offenlegung von Unterlagen und Auskünften einzufordern und das Unternehmen pflichtweise als kritische Infrastruktur zu registrieren. Kommt es bei einem registrierten KRITS-Betreiber zu einer Störung der Informationssicherheit, muss diese umgehend gemeldet werden.

Was sollten KRITIS-Betreiber bei der Nutzung von Cloud-Diensten beachten?

Aufgrund der strengen Regularien war KRITIS-Betreibern die Nutzung von Cloud-Diensten lange Zeit vollständig verwehrt. Diese Vorgaben wurde jedoch inzwischen aufgehoben und nun dürfen auch KRITIS-Unternehmen unter speziellen Bedingungen von der Microsoft Cloud profitieren. Bei der Planung ihrer Cloud-Strategie, empfiehlt es sich für KRITIS-Unternehmen im Vorfeld zu definieren, welche Dienstleistungen in der Cloud realisiert werden sollen. Hauptaugenmerk sollte dabei auf der Verfügbarkeit und Sicherheit der genutzten Dienste liegen. Betreiber von KRITIS-Infrastrukturen müssen sich jedoch darüber im Klaren sein, dass sie die Verantwortlichkeiten im Hinblick auf Datenschutz und Compliance nicht an die Betreiber von Cloud-Rechenzentren übertragen können, sondern selbst für die Umsetzung datenschutzkonformer Regularien zuständig sind.

Bußgelder bei Versäumnissen

Verstöße können Betreibern kritischer Infrastrukturen teuer zu stehen kommen. So erweitert das KRITIS 2.0 noch einmal die Bußgeldtatbestände sowie die Ahnungshöhe erheblich. In Abhängigkeit des jeweiligen Tatbestands können gemäß § 14 Abs. 5 BSIG Bußgelder von bis zu 2 Mio. Euro verhängt werden. Des Weiteren können nach Zuwiderhandlungen gegen Anordnungen des BSI zur Wiederherstellung oder der Gefahrenabwehr nach § 14 Abs. 5 BSIG mit Verweis auf § 30 Abs. 2 Satz 3 OWiG gegen juristische Personen Bußgelder von bis zu 20 Mio. Euro verordnet werden.

DIE DATENSCHUTZ-FOLGEABSCHÄTZUNG

DIE DATENSCHUTZ-FOLGEABSCHÄTZUNG

Seit dem Inkrafttreten der DSGVO greifen bei der Verarbeitung von personenbezogenen Daten verschärfte Anforderungen. Was früher im Rahmen des alten Bundesdatenschutzgesetzes noch als Vorabkontrolle bekannt war, wurde im Zuge der Datenschutz-Grundverordnung zur Datenschutz-Folgeabschätzung. Insbesondere für kleine und mittlere Unternehmen stellt die Folgenabschätzung eine Herausforderung dar, da es sich hierbei um einen umfangreichen und aufwändigen Prozess handelt. Allerdings ist nicht jedes Unternehmen zu einer Datenschutz-Folgenabschätzung verpflichtet.

Wann muss eine Datenschutz-Folgeabschätzung vorgenommen werden?

Nach Art. 35 Abs. 1 DSGVO ist eine DSFA grundsätzlich immer dann durchzuführen, wenn:
„(…) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge [hat]“.

Vor der Datenschutz-Folgeabschätzung wird zunächst eine Schwellwertanalyse durchgeführt. Mit dieser wird festgestellt, ob die Datenverarbeitung einem hohen Risiko unterliegt. Darüber hinaus werden in Art. 35 Abs. 3 DSGVO Regelbeispiele genannt, bei denen eine Durchführungspflicht besteht:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen.
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO.
- systematische weiträumige Überwachung öffentlich zugänglicher Bereiche.

Ablauf der Datenschutzfolgeabschätzung am Beispiel der Funktion „Sprache zu Text“ in Microsoft Teams

Eine Datenschutz-Folgeabschätzung, wird durchgeführt, um die Auswirkungen einer geplanten Datenverarbeitung auf den Datenschutz und die Privatsphäre von betroffenen Personen zu bewerten. Wir erläutern den Ablauf der Datenschutzfolgeabschätzung am Beispiel der von Microsoft kürzlich neu integrierten Teams-Funktion „Sprache zu Text“. Mit der Funktion sollen Videokonferenzen barrierefrei und leichter zu verfolgen sein. Dazu werden Machine Learning und KI eingesetzt. Im Allgemeinen beinhaltet die Durchführung einer Datenschutz-Folgeabschätzung die folgenden Schritte:

SCHRITT 1

BESCHREIBUNG DER VERARBEITUNGSVORGÄNGE

Erläuterung der Art, des Umfangs, des Zwecks und der Notwendigkeit der Verarbeitung personenbezogener Daten.

Zweck: Umwandlung gesprochener Sprache in geschriebenen Text in Microsoft Teams, um die Kommunikation zu erleichtern, Transkripte zu erstellen und die Zugänglichkeit zu verbessern.

Datenverarbeitung: Audioaufnahmen von Benutzern werden erfasst, an Microsoft-Server gesendet und in Text umgewandelt.

Notwendigkeit: Die Verarbeitung ist notwendig, um den Kommunikationsbedürfnissen der Nutzer gerecht zu werden und den Zugang zu Informationen für Menschen mit Hörbehinderungen zu erleichtern.

Verhältnismäßigkeit: Die Verarbeitung steht in einem angemessenen Verhältnis zum angestrebten Zweck.

SCHRITT 2

IDENTIFIZIERUNG VON RISIKEN

Analyse der potenziellen Risiken für die Rechte und Freiheiten der betroffenen Personen, die aus der Verarbeitung personenbezogener Daten resultieren.

Datenschutzrisiken: Verletzung der Vertraulichkeit und Integrität von personenbezogenen Daten, Missbrauch von Audioaufnahmen, unerwünschte Profilbildung und Entscheidungsfindung.

SCHRITT 3

BEWERTUNG DER RISIKEN

Einschätzung der Wahrscheinlichkeit und Schwere der identifizierten Risiken sowie ihrer möglichen Auswirkungen auf die betroffenen Personen.

Wahrscheinlichkeit: Mittel

Schwere: Hoch

SCHRITT 3

MINDERUNG VON RISIKEN

Identifizierung und Implementierung geeigneter technischer und organisatorischer Maßnahmen zur Risikominderung und zum Schutz der personenbezogenen Daten.

Datensparsamkeit: Die Audioaufnahmen werden nur so lange gespeichert, wie dies zur Erfüllung des Zwecks erforderlich ist.

Pseudonymisierung: Soweit möglich, sollten die Audioaufnahmen von den Benutzeridentitäten getrennt und pseudonymisiert werden.

Verschlüsselung: Audioaufnahmen und Transkripte werden während der Übertragung und Speicherung verschlüsselt.

Zugriffskontrolle: Nur autorisierte Mitarbeiter haben Zugriff auf die Audioaufnahmen und Transkripte.

Transparenz: Benutzer werden über die Verwendung ihrer Daten und ihre Rechte in Bezug auf die Verarbeitung informiert.

Datenschutz durch Design und Voreinstellungen: Die Sprache-zu-Text-Funktion sollte standardmäßig deaktiviert sein und nur aktiviert werden, wenn der Benutzer zustimmt.

SCHRITT 4

KONSULTATION DER DATENSCHUTZ-BEHÖRDE

Bei hohen Restrisiken nach der Risikominderung kann es erforderlich sein, die zuständige Datenschutzbehörde zu konsultieren, bevor die Verarbeitung personenbezogener Daten fortgesetzt wird.

Konsultation von Datenschutzexperten und betroffenen Personen (wie Benutzer oder Mitarbeiter) bei der Entwicklung und Implementierung der Funktion.

SCHRITT 5

REGELMÄSSIGE ÜBERPRÜFUNG

Eine DSFA sollte in regelmäßigen Abständen überprüft und aktualisiert werden, um Veränderungen in den Verarbeitungsvorgängen oder neuen Risiken Rechnung zu tragen.

Zu beachten ist hierbei, dass die genaue Vorgehensweise und der Umfang einer Datenschutz-Folgeabschätzung je nach spezifischer Situation und geltenden Datenschutzbestimmungen variieren können. In einigen Fällen kann es erforderlich sein, externe Experten hinzuzuziehen, um eine umfassende Bewertung durchzuführen.

MASSNAHMEN FÜR DEN DATENSCHUTZ-KONFORMEN EINSATZ VON MICROSOFT 365

Die cloudbasierte Version von Microsoft 365 ist in vielen Unternehmen ein etablierter Standard. Bei den Datenschutz-Aufsichtsbehörden stand die Plattform jedoch auch immer wieder in der Kritik. Verantwortliche in Unternehmen sind deshalb dazu angehalten, risikominimierende Maßnahmen sowie datenschutzfreundliche Voreinstellungen vorzunehmen.

Überwachung der Service Principals im ADD

Service Principals sind technische Identitäten, mithilfe derer Automatismen entwickelt werden können, die gegebenenfalls auf Daten in Microsoft 365 zugreifen.

Ist das Management dieser Identitäten nicht ausreichend gewährleistet, erhöht sich auch das Risiko von Datenabflüssen und es ergib sich ein Compliance-Risiko. Daher sollten die Aktivitäten der eingesetzten Service Principals regemäßig überprüft werden.

Anzahl der Admins im Blick behalten

Die Menge der globalen Administratoren sollte im Verhältnis zu allen Benutzern in der Organisation stehen. Eine hohe Anzahl an Global Admins steigert das Sicherheitsrisiko, da jeder Admin in seiner Umgebung ein ideales Ziel für Angreifer darstellt und unter Umständen nicht mehr gewährleistet werden kann, dass die Global Admins verantwortungsvoll mit ihrer Rolle umgehen. Dagegen kann eine zu niedrige Anzahl an Global Admins dazu führen, dass die Rechteverwaltung nicht mehr ordnungsgemäß durchgeführt werden kann.

Ernennung eines Compliance Administrators

Compliance Administratoren besitzen Verwaltungsberechtigungen innerhalb von Office 365 Security & Compliance Center und dem Exchange Admin Center.
Ist diese Rolle im Unternehmen nicht vergeben, ergeben sich Risiken für die Sicherstellung des Betriebs, wenn es zu Vorfällen wie z.B. Datenschutzverstößen kommt

EU Data Boundary für die Microsoft Cloud

USeit dem 1. Januar 2023 bietet Microsoft Kunden die Möglichkeit zur Speicherung und Verarbeitung ihrer Daten innerhalb der EU-Datengrenze für Microsoft 365, Azure, Power Platform und Dynamics 365. Damit erweitert Microsoft die bestehenden Maßnahmen zur lokalen Speicherung und Verarbeitung. So werden bestimmte Daten nur in der EU verarbeitet und die Wahrscheinlichkeit von Zugriffen aus den USA durch Microsoft verringert. Die Funktion ist jedoch derzeit nur für bestimmte Module konzipiert und schließt externe Wartungszugriffe nicht aus.

Zur Gewährleistung von Compliance und Datenschutz, sind darüber hinaus folgende Voreinstellungen zu empfehlen:

- Einstellung „weder noch“ („neither“) bei Diagnosedaten in MS 365;
- Einstellung „Diagnosedaten aus (Sicherheit)“ („Diagnostic data off (Security)“) in Windows 10;
- Deaktivieren der Programme zur Verbesserung der Kundenerfahrung
- Deaktivieren von Aktivitätsberichten
- Deaktivieren von „Senden von persönlichen Informationen an Microsoft, um Office zu verbessern“ und „Office die Verbindung mit Microsoft-Onlinediensten erlauben, um für Ihren Standort und Ihre Voreinstellungen relevante Funktionen bereitzustellen“ in Microsoft Office

PRW®Compliance Set M:365

Mit dem PRW®Compliance Set M:365 liefern wir ein ideales Instrument, um Microsoft 365 datenschutzkonform absichern und nutzen zu können. Wir bedienen uns der, von PRW entwickelten, Software und ergänzen unser jahreslanges Know How im Umfeld der Compliance für M365. So entsteht eine Lösung, mit der die bestehende Microsoft 365-Umgebung des Anwenderunternehmens im Hinblick auf Datenschutz, Informationssicherheit und Wahrung der Mitbestimmungsrechte umfassend analysiert werden kann. Die technische und rechtliche Analyse umfasst dabei nicht nur eine Darstellung der tatsächlich genutzten IT-Umgebung, sondern gibt auch detaillierte technische und rechtliche Handlungsempfehlungen. Die technische Analyse, die von den Partnern der PRW Legal Tech GmbH durchgeführt wird, umfasst eine Ist-Analyse der bestehenden Microsoft-365-Umgebung und erfolgt mittels einer eigens von der PRW Legal Tech GmbH entwickelten Software. Diese scannt den gesamten Tenant und zeigt auf, wie dieser konfiguriert ist, mit dem Ziel, Schwachstellen und deren Behebung aufzuzeigen.

HANDLUNGS-EMPFEHLUNGEN FÜR COMPLIANCE & DATENSCHUTZ IN EINER EVERGREEN IT

HANDLUNGSEMPFEHLUNGEN FÜR COMPLIANCE & DATENSCHUTZ IN EINER EVERGREEN IT

In den Produkten von Microsoft 365 gibt es fortlaufend Aktualisierungen und Updates, sodass es schwer sein kann, den Überblick zu behalten. Dabei muss die IT-Abteilung schnell entscheiden, ob neue Funktionen datenschutzkritisch sind. Es stehen viele Entscheidungen in kurzer Zeit an, die gerade bei kleineren IT-Abteilungen ohne Evergreen Manager und enger Abstimmung mit IT-Security und Datenschutz eine Herausforderung darstellen.

Hier sind einige wichtige Schritte für ein systematisches Vorgehen, die dabei helfen können:

- Kenntnis der Compliance-Anforderungen: Dazu gehören gesetzliche Bestimmungen, branchenspezifische Vorschriften und interne Richtlinien.

- Überprüfung der Evergreen-Strategie: Die Evergreen-Strategie sollte Mechanismen enthalten, um sicherzustellen, dass Software, Betriebssysteme und andere IT-Komponenten kontinuierlich aktualisiert und auf dem neuesten Stand gehalten werden, um Sicherheitslücken zu schließen und Compliance-Risiken zu minimieren.

- Implementierung eines Change-Management-Prozesses: Im Zuge des Change-Management-Prozesses sollten Änderungen an der IT-Infrastruktur kontrolliert und dokumentiert werden. Dies beinhaltet die Überprüfung und Genehmigung von Änderungen sowie die Durchführung von Tests und Risikobewertungen, um unvorhergesehene Auswirkungen auf die Compliance zu vermeiden.

- Regelmäßige Überprüfung und Audits: Um mögliche Schwachstellen zu identifizieren und zu beheben sollten sowohl technische Aspekte als auch relevante Prozesse und Richtlinien überprüft werden.

- Sicherheitsmaßnahmen implementieren: Dazu gehören die Implementierung von Zugriffskontrollen, Verschlüsselungstechnologien, Sicherheitsüberwachung und Datenschutzmaßnahmen.

- Schulung und Sensibilisierung der Mitarbeitenden: Sensibilisierung der Mitarbeitenden über ihre Verantwortung bei der Umsetzung von Sicherheitsmaßnahmen und bei der Einhaltung der Richtlinien.

- Externe Partner und Dienstleister einbeziehen: Sind externe Partner oder Dienstleister in die Evergreen-IT-Umgebung eingebunden, muss sichergestellt werden, dass sie die Compliance-Anforderungen verstehen und entsprechende Maßnahmen ergreifen, um diese einzuhalten.

RECHTLICHE BEWERTUNG DES MICROSOFT 365 TENANTS

Im Rahmen unseres Compliance Packs in Zusammenarbeit mit der PRW Group bieten wir einen halbjährlichen Scan Ihres gesamten Tenants an. Dazu wird auf Basis der Software „PRW® Compliance Set: M365“ eine vollständig softwarebasierte, technische Analyse eines bestehenden Microsoft 365 Tenants durchgeführt. Unsere Experten leiten das Projekt, begleiten den technischen Scan, beraten zu notwendigen technischen und organisatorischen Maßnahmen und unterstützen aktiv bei deren Umsetzung und Verankerung im Unternehmen. Die rechtliche Bewertung auf Basis der Analyseergebnisse erfolgt durch die PRW Group.

MICROSOFT 365 PLATTFORM

MICROSOFT 365 PLATTFORM

Microsoft Teams ist ein chatbasierter zentraler Arbeitsbereich innerhalb der Microsoft-365-Umgebung. Das Tool dient der digitalen Unterstützung von effektiver Kommunikation und Kollaboration bei der Teamarbeit.
Microsoft Teams ist damit mehr als nur eine Lösung für Chats und digitale Meetings, sondern vielmehr das Frotend für die Nutzung der gesamten Microsoft-365-Plattform und bietet Zugriff auf viele andere Microsoft-365-Dienste, z.B. SharePoint Online, Office Groups, OneDrive oder auch auf den Microsoft Planner.

DATENSCHUTZRISIKEN BEI MICROSOFT TEAMS

Der Einsatz von Microsoft Teams birgt für Unternehmen zahlreiche Vorteile, jedoch entstehen dabei auch Risiken für den Datenschutz. Für Unternehmen ist es deshalb wichtig, diese Risiken zu verstehen und entsprechende Maßnahmen zu ergreifen, um den Schutz personenbezogener Daten zu gewährleisten:

- Datenspeicherung: Microsoft Teams ermöglicht die Speicherung von Chat-Nachrichten, Dateien, Anrufaufzeichnungen und anderen Daten in der Cloud. Hier besteht die Gefahr, dass sensible Informationen, wenn sie nicht angemessen geschützt werden, von unbefugten Personen eingesehen oder kompromittiert werden können. Unternehmen sollten daher sicherstellen, dass geeignete Zugriffskontrollen und Verschlüsselungen angewendet werden, um die Datensicherheit zu gewährleisten.

- Datenübertragung: Beim Einsatz von Teams werden Daten über das Internet übertragen. Werden diese Daten während der Übertragung nicht angemessen verschlüsselt, kann dies den Schutz dieser Daten gefährden. Um dieses Risiko zu mindern, sollten Unternehmen sicherstellen, dass eine sichere Kommunikationsinfrastruktur verwendet wird, z. B. durch die Ver-

wendung von verschlüsselten Verbindungen (HTTPS) und Virtual Private Networks (VPNs).

- Externe Teilnehmer: Microsoft Teams ermöglicht die Zusammenarbeit mit externen Partnern und Kunden über Gastzugriffsfunktionen. Hierbei empfiehlt es sich für Unternehmen Berechtigungs- und Zugriffskontrollen zu implementieren, um den Zugriff auf sensible Daten auf autorisierte Benutzer zu beschränken.

- Drittanbieter-Integrationen: Bei der Verwendung solcher Integrationen besteht das Risiko, dass Drittanbieter Zugriff auf die dort gespeicherten Daten erhalten. Unternehmen sollten daher die Datenschutzrichtlinien von Drittanbietern überprüfen und sicherstellen, dass sie den geltenden Datenschutzstandards entsprechen.

Um die Datenschutzrisiken beim Einsatz von Microsoft Teams zu mindern, empfiehlt es sich Datenschutzrichtlinien und -verfahren zu implementieren, Schulungen für Mitarbeitende anzubieten, um den sicheren Umgang mit Daten zu fördern und regelmäßige Überprüfungen der Sicherheitskonfigurationen und Einstellungen in Teams durchzuführen. Durch angemessene Maßnahmen können die Privatsphäre und den Schutz personenbezogener Daten gewährleistet und die Risiken minimiert werden.

DATENSCHUTZFREUNDLICHE EINSTELLUNGEN FÜR MICROSOFT TEAMS

Microsoft Teams bietet verschiedene datenschutzfreundliche Voreinstellungen, die Unternehmen dabei unterstützen, den Schutz personenbezogener Daten zu gewährleisten. Diese Einstellungen sind darauf ausgerichtet, Datenschutzprinzipien wie Datensparsamkeit, Zugriffsbeschränkungen und Transparenz zu fördern. Geeignete Maßnahmen sind zum Beispiel:

Standardmäßige Datenschutzeinstellungen Microsoft Teams enthält standardmäßig eine Reihe von Datenschutzeinstellungen, die den Schutz personenbezogener Daten unterstützen. Dazu gehören z. B. die Möglichkeit, Aufzeichnungen von Besprechungen zu deaktivieren, das Teilen von Bildschirmen einzuschränken und Benutzerdaten in der Cloud zu verschlüsseln.

TEAMS APP STORE

Häufig wird übersehen, dass im Teams App Store auch kostenlose Apps zum Datentransfer verfügbar sind. Google-Drive, Dropbox und viele deutlich unbekanntere Anbieter, wie zum Beispiel Box, sind nur einige Beispiele für Apps dieser Art. Darüber hinaus sind einige Apps wie z.B. Mindmeister (Whiteboard) im Standard erlaubt, jedoch liegen die

Speicherorte der Daten außerhalb der Microsoft-365-Umgebung. Durch die Möglichkeit des Datenabflusses ergeben sich dabei speziell im Umfeld der DLP (Data Los Prevention) Risiken für den Datenschutz. Deshalb empfiehlt es sich, Richtlinien für die Nutzung des Teams App Stores festzulegen und eine Black List für risikoreiche Apps zu erstellen.

SMART REPLY

Microsoft Teams nutzt Machine Learning um "Smart Reply"- Nachrichten mit Hilfe von Cognitive Services zu verbessern. Diese Funktion kann auch außerhalb der Europäischen Union stattfinden und ist somit nicht mit der DSGVO vereinbar. Unternehmen sollte diese Funktion in den Einstellungen deaktivieren.

TEAMS STATUS

Der Anwesenheitsstatus der User ist im Standard für jeden jederzeit einsehbar. Da es sich um personenbezogene Daten handelt, ergibt sich ein Datenschutzrisiko nach DSGVO. Außerdem entsteht dadurch Möglichkeit von außerhalb der Organisation Profile der Benutzer zu erstellen (typische An- und Abwesenheiten, Urlaube, freie Tage, etc.). Dies stellt auch ein akutes Risiko für erfolgreiche Phishing-Angriffe dar. Wir empfehlen deshalb, den Anwesenheitsstatus für Externe zu deaktivieren, sodass nur noch Benutzer innerhalb des Unternehmens und Gäste den Anwesenheitsstatus einsehen können.

GASTZUGRIFFSKONTROLLE

Unternehmen können die Einstellungen für den Gastzugriff in Microsoft Teams steuern, um den Zugriff externer Teilnehmer zu verwalten. Sie können festlegen, ob Gäste Dateien hochladen, bearbeiten oder löschen können und welche Kommunikationsfunktionen für sie verfügbar sind. Dies ermöglicht eine granulare Kontrolle über den Zugriff auf sensible Informationen.

FAZIT

FAZIT

Microsoft 365 bietet eine Vielzahl von Datenschutz- und Compliance-Funktionen, die Unternehmen dabei unterstützen, ihre Daten zu schützen und rechtliche Anforderungen einzuhalten. Durch die Implementierung geeigneter Maßnahmen und Best Practices können Unternehmen ihre Daten effektiv schützen. Ein zentraler Aspekt ist die Einhaltung der Datenschutzgrundverordnung (DSGVO) und anderer relevanter Datenschutzgesetze. Microsoft hat hierzu umfangreiche Funktionen und Kontrollen in seine Dienste integriert. Dazu gehören Datenschutzvereinbarungen, Vertragszusätze und Transparenzberichte, die Unternehmen dabei unterstützen, die Datenschutzprinzipien umzusetzen. Die Datenschutzfunktionen von Microsoft 365 umfassen auch datenschutzfreundliche Einstellungen und Konfigurationen, mit denen Unternehmen die Kontrolle über ihre Daten behalten können.

Es ist jedoch wichtig zu beachten, dass Unternehmen auch die Verantwortung tragen, um Datenschutz- und Compliance-Ziele zu erreichen. Dies umfasst die gewissenhafte Konfiguration der Einstellungen innerhalb Microsoft 365, die Schulung der Mitarbeitenden sowie die regelmäßige Überprüfung und Aktualisierung der Datenschutz- und Compliance-Maßnahmen. Auch die Zusammenarbeit mit Datenschutzexperten und Compliance-Spezialisten kann dabei helfen, eine optimale Nutzung von Microsoft 365 im Einklang mit Datenschutz- und Compliance-Bestimmungen zu gewährleisten.

JETZT KONTAKT AUFNEHMEN!

Haben Sie Fragen oder wünschen eine persönliche Beratung? Lassen Sie uns über ihr Projekt sprechen!

Ihr Ansprechpartner:
Daniel Wintermeier
Mail: daniel@provectus.de
Tel.: +49 (0) 89 710 409 20

Schon gesehen?
In unseren **Quick Assessment** erfahren Sie in nur wenigen Minuten wo Sie mit diesem Thema stehen.
provectus.de/complaince-check