YOUR KEY
TO DIGITAL
FREEDOM

–

DATENSCHUTZ FÜR MICROSOFT 365

WHITEPAPER

DRACOON

INHALTSVERZEICHNIS

INHALTSVERZEICHNIS

1. WIE SETZE ICH GÄNGIGE CLOUD-SPEICHER-PRODUKTE WIE MICROSOFT ONEDRIVE, OUTLOOK ODER TEAMS GDPR-KONFORM EIN?

Die Nutzung von Cloud-Diensten hat in den letzten Jahren stark zugenommen, sowohl im privaten Bereich als auch in Unternehmen. Die Vorteile sind nicht von der Hand zu weisen, denn die Cloud stellt eine zentrale Sammelstelle für Daten und Dokumente dar, auf die unabhängig von Ort und Gerät zugegriffen werden kann. Doch wie verhält sich eine Cloud-Lösung wie z.B. Microsoft OneDrive im Kontext des Datenschutzes?

2. DER EINSATZ VON MICROSOFT ONEDRIVE VERSUS GDPR-KONFORMITÄT

Benutzer von OneDrive sollten auf jeden Fall eines bedenken: Hier werden einem amerikanischen Dienstleister (Microsoft) eigene oder firmeneigene Daten anvertraut, die zum Teil sehr persönlich sind oder besonderen Schutz benötigen. Microsoft hat seinen Sitz in den USA. Auch wenn es viele Angebote für Serverstandorte innerhalb der EU gibt, kann nicht ausgeschlossen werden, dass auch Server und Mitarbeiter in den USA Zugriff auf die anderen Serverstandorte haben, beispielsweise zu Supportzwecken. Aufgrund des CLOUD Acts und der Schrems II-Entscheidung des EuGH sollte man sich daher genau überlegen, ob man seine Daten tatsächlich bei amerikanischen Cloud-Betreibern speichern möchte.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ging im Juli letzten Jahres noch einen Schritt weiter. Sie beschloss mit einer knappen Mehrheit von 9 zu 8 Gegenstimmen, dass eine datenschutzkonforme Nutzung von Microsoft Office 365 (und damit auch von MS OneDrive) nicht möglich sei. Die DSK führte insbesondere folgende Gründe an:

- **Fehlende Details**
  Die Beschreibung der Verarbeitung in den Online-Dienstbedingungen und in der Auftragsabwicklung ist nicht detailliert genug, um beurteilen zu können, ob die Verarbeitung durch Microsoft zulässig ist.

- **Keine Rechtsgrundlage für Telemetrie**
  Für die Übermittlung von Telemetrie-Diagnosedaten an Microsoft gibt es keine Rechtsgrundlage.

- **Ungenauer Hinweis auf mögliche Übertragungen**
  Der vertragliche Vorbehalt der Weitergabe von Daten in gesetzlich vorgeschriebenen Fällen war zu abstrakt.

Die Entscheidung der DSK kann aber auch kritisch gesehen werden, da sie auf Basis allgemeiner Dokumente und ohne konkreten technischen Einblick getroffen wurde. Sowohl Office 365 als auch Microsoft 365 bestehen jedoch aus einem Bündel verschiedener Produkte und Funktionen, die sich fast wöchentlich ändern. In der Praxis wird die Beurteilung der Zulässigkeit daher immer von der konkreten Nutzung von Microsoft 365 und damit

auch von OneDrive abhängen. Die Einschätzung der DSK hingegen ist auf dem Stand von Januar 2020 und stellt somit nur eine Momentaufnahme dar. Es ist daher wohl fraglich, ob und inwieweit die beanstandeten Punkte nicht bereits angepasst wurden.

Ist OneDrive für Unternehmen geeignet?

In den meisten Fällen wird Microsoft OneDrive wohl als Cloud-Dienst für Unternehmen im Rahmen einer bestehenden Microsoft-Lizenz in Frage kommen. Bevor man es nutzt, sollte man sich zwei entscheidende Fragen stellen: Werden persönliche Daten in die Microsoft-Cloud hochgeladen und wie geht man mit dem Serverstandort in den USA um?

Aus rechtlicher Sicht lässt sich nicht abschließend sagen, ob die Nutzung von OneDrive zulässig ist oder nicht. In der Praxis wird es daher immer auf eine Bewertung der eigenen Risikosituation des Unternehmens ankommen. Die Vorteile (z.B. OneDrive wird bereits genutzt und der wirtschaftliche Nutzen) müssen gegen die Nachteile (z.B. Risiken hinsichtlich der DSGVO-Compliance verbunden mit dem Risiko von Bußgeldern) abgewogen werden. Nur wenn keine personenbezogenen Daten in der Cloud gespeichert sind, kann OneDrive bedenkenlos im Kontext der DSGVO genutzt werden. Wenn man noch das Thema Wirtschaftsspionage mit einbezieht, sollte man auch bei nicht personenbezogenen kritischen Unternehmensdaten ernsthaft überlegen, ob man diese einem amerikanischen Cloudbetreiber anvertrauen möchte. Eine Alternative wäre der Aufbau einer eigenen Firmen-Cloud oder die Nutzung eines Produkts wie z.B. DRACOON.

MS OneDrive vs. Apple iCloud - Wie schlägt sich der Konkurrent?

Lassen wir den Blick auf die „fruchtige" Konkurrenz von Microsoft OneDrive schweifen. Nachdem Apple seinen Cloud-Dienst lange Zeit ausschließlich für die private Nutzung angeboten hat (um damit die Anwendung der DSGVO zu umgehen, die nach Art. 2 Abs. 2 lit. c) im privaten Bereich nicht gilt), gibt es nun die Variante iCloud Business Manager.

Der größte Kritikpunkt an der Business-Version von iCloud - neben der Tatsache, dass es sich um einen amerikanischen Dienstleister handelt - ist folgender Punkt: Apple behauptet, ein Prozessor zu sein. Verschiedene Regelungen im Vertrag deuten jedoch auf das Gegenteil hin. So behält sich Apple das Recht vor, den Zugriff des Nutzers auf seine (!) Daten nach Vertragsende zu sperren und seine Daten ohne vorherige Herausgabe zu löschen. Dies verstößt eindeutig gegen die Bestimmungen des Artikels 28 der GDPR.

Was sind die sichersten Alternativen zu OneDrive?

Die Folge: Nicht-europäische Cloud-Dienste - ob Microsoft OneDrive, Apples iCloud, Google oder Amazon Drive - haben alle das gleiche Problem: Ihre Anbieter sitzen in den USA. Seit der EuGH in seinem Schrems-II-Urteil das EU-US Privacy Shield als Rechtsgrundlage für den Austausch personenbezogener Daten mit den USA gekippt hat, ist ein angemessenes Datenschutzniveau beim Datentransfer nicht mehr gewährleistet. Wie mit dieser Entscheidung und den daraus resultierenden Folgen und Risiken umzugehen ist, muss im Einzelfall abgewogen werden.

Wer jedoch auf der sicheren Seite sein will, sollte sich entweder für die Einrichtung einer eigenen Firmen-Cloud oder für einen Cloud-Anbieter entscheiden, der seinen Sitz und seine Server ausschließlich in der EU hat. Ebenso sollten bei der Wahl sowohl die individuellen Bedürfnisse als auch die Schutzmaßnahmen des Anbieters berücksichtigt werden. Hier können z. B. Themen wie die Synchronisation von Daten, Design und Usability, kollaboratives Arbeiten, die Anzahl der Nutzer, Verschlüsselung und das Datenschutzniveau sowie die Kosten im Verhältnis zur Speicherkapazität berücksichtigt werden.

In Deutschland gibt es jedoch viele gute Alternativen zu OneDrive. Die Anbieter von „bdrive", „DRACOON", „IONOS HiDrive", „Magenta Cloud" und „Your Secure Cloud" zum Beispiel haben ihre Serverstandorte in Deutschland und sind nach ISO/ IEC 27001 zertifiziert.

3. DATENSCHUTZ IN MICROSOFT TEAMS – WIE FUNKTIONIERT ES RICHTIG?

Microsoft 365 ist die gängigste Datenverarbeitungssoftware auf dem Markt. Microsoft Teams ist nicht zuletzt durch die Corona-Pandemie für Unternehmen, Schulen und Privatanwender zu einem zentralen Ort der Zusammenarbeit geworden. Die Zukunft des digitalen Arbeitsplatzes hat längst begonnen. Das Thema Datenschutz darf dabei aber nicht außer Acht gelassen werden.

Datenschutz in MS Teams: Wer greift auf Ihre Daten zu?

Problematisch gestalten sich bislang für deutsche und europäische Nutzer die rechtssichere Speicherung und der Austausch von sensiblen Daten. Tauscht man Dokumente in MS Teams aus, kann auf diese durch US-amerikanische Behörden zugegriffen werden. Das bedeutet, dass Daten ohne die Nutzung einer Zusatzlösung in MS Teams nicht sicher sind.

Ist Microsoft Teams datenschutzkonform?

Office 365 gehört zu unserem Alltag und steht stellvertretend für unkomplizierte, flexible Zusammenarbeit, egal von welchem Ort. Besonders MS Teams erfreut sich inzwischen großer Beliebtheit und bringt Menschen rund um den Globus zusammen. Allerdings sollten europäische Unternehmen genau hinsehen beim Einsatz von Office 365, denn das Thema Datenschutz darf nicht zu kurz kommen. Ein Zugriff von Unternehmen mit Hauptsitz außerhalb der EU ist möglich. Allerdings kann man durch eine Erweiterung um eine Datenaustauschlösung im Teams App Store die Datensicherheit wieder gewährleisten.

Wo ist der geografische Speicherort von Kundendaten in MS Teams?

Wenn ein Unternehmen zu einem US-amerikanischen Mutterkonzern gehört, greift der US-amerikanische CLOUD ACT. Diese Regelung führt zu einem Konflikt mit der EU-Datenschutzgrundverordnung (DSGVO). Denn ohne Rechtshilfeabkommen dürfen personenbezogene Daten schon DSGVO-bedingt nicht an US-Behörden übergeben werden. Mit Lösungen wie DRACOON oder anderen Anbietern für den sicheren und besonders DSGVO-konformen Austausch von Daten, also effektivem Filesharing, bleibt die hohe Flexibilität der Microsoft Produkte erhalten. DRACOON lässt sich dabei zum Beispiel für MS Teams einfach im Teams App Store herunterladen.

Microsoft Teams nutzen viele Unternehmen täglich zur Zusammenarbeit. Wie man die Lösung einsetzen kann, welche Daten Teams speichert und wieso das Thema DSGVO-konformer Dateiaustausch ein Problem darstellt, erklären wir im nächsten Abschnitt.

Wozu kann man Teams nutzen?

- Über Microsoft Teams lassen sich Besprechungen, Chats, Notizen und Anhänge digital organisieren und bereitstellen. Der Chat ermöglicht eine Kommunikation mit einzelnen Kollegen, Gruppen oder dem vollständigen Team. Das Tool erleichtert das Arbeiten im Homeoffice, aber gleichermaßen auch den Austausch im klassischen Büroalltag. MS Teams ist in der Microsoft 365-Suite mit Microsoft Office und Skype bzw. Skype for Business und OneDrive integriert. Alle Tools sind für die Zusammenarbeit von Teams ausgerichtet.

Welche Daten speichert MS Teams?

- Bei der täglichen Verwendung von Microsoft Teams werden einige Daten generiert. Dies sind alles offensichtliche Dinge, wie Profildaten, E-Mail-Adresse und (falls angegeben) Profilbild und Telefonnummer. Darüber hinaus gibt es Video- und Audiodateien wie Voicemail oder Aufzeichnungen sowie die Informationen, die in Chats oder privaten Nachrichten übermittelt werden. Natürlich kann man Dateien auch privat speichern oder gemeinsam in einem Team bearbeiten. Wenn all diese persönlichen Daten zwischen verschiedenen Geräten, Benutzern oder zwischen Rechenzentren übertragen und in Rechenzentren gespeichert werden, werden sie alle von Microsoft gespeichert und mit Standardtechnologien verschlüsselt.

Warum braucht man eine externe Lösung um Daten in Teams abzusichern?

- Die EU-DSGVO, die im Mai 2018 eingeführt wurde, schreibt sehr genau vor, wie Daten in Deutschland und Europa gespeichert und verarbeitet werden dürfen. Seither gelten noch strengere Regularien, und Verstöße werden mit hohen Bußgeldern sanktioniert. Der CLOUD Act jedoch verpflichtet Unternehmen mit Sitz in den USA und gleichermaßen Unternehmen, die zu einem US-amerikanischen Mutterkonzern (wie beispielsweise Microsoft) gehören, dazu, sämtliche Daten zu Ermittlungszwecken bereitzustellen, sofern dies als notwendig erachtet wird.

Durch den CLOUD Act ist für diese Datenherausgabe nicht einmal ein gesonderter Beschluss notwendig. Er verpflichtet US-Unternehmen sogar dann zur Herausgabe, wenn lokale Gesetze am Ort des Datenspeichers das verbieten. Auf diese Art und Weise stellt die US-Regierung auch den Zugriff auf ausländische Server sicher. Und dem müssen sich auch europäische Unternehmen beugen, sofern sie ihre Daten nicht anderweitig absichern. In Europa hingegen untersagt die EU-DSGVO eine Herausgabe von personenbezogenen Daten ohne ein gültiges Rechtsabkommen. Deshalb tritt jedes Unternehmen, das unter die Regularien der EU-DSGVO fällt, in einen Konflikt, wenn es Microsoft-Produkte einsetzt. Denn jede Nutzung von MS Teams kollidiert mit der EU-DSGVO,

sofern dort Daten über die integrierten Dienste gespeichert werden. Um dies zu umgehen, sollten Daten, die in MS Teams verwendet werden, speziell abgesichert und DSGVO-konform extern (z. B. in DRACOON) gespeichert werden.

4 Vorteile für den Schutz Ihrer Daten in MS Teams:

MS Teams aufgrund von Sicherheitsbedenken nicht zu nutzen, wäre ein realitätsferner Lösungsansatz. Deshalb bieten externe Applikationen, die DSGVO-konform arbeiten, Abhilfe. Der Einsatz solcher Filesharing-Plattformen bietet aber mehr Vorteile als auf den ersten Blick ersichtlich.

- **1. Schützen Sie Ihre Daten bei Verwendung von Microsoft 365: Keines Ihrer Dokumente wird an Microsoft oder Dritte weitergegeben. Sie können GDPR-konform Dokumente in MS Teams austauschen.**
- **2. Vermeiden Sie Duplikate und sparen Sie Zeit: Durch das Austauschen von Datei-Links wird sichergestellt, dass immer an der Original-Version der Datei gearbeitet wird. Sie können Dateien direkt in Microsoft Teams suchen und freigeben.**
- **3. Erfüllen Sie Compliance-Richtlinien automatisch: Mit der datenschutzfreundlichen Technikgestaltung (Privacy by Design) sowie Voreinstellung (Privacy by Default) arbeiten Sie als Benutzer automatisch datenschutzkonform und erfüllen alle Compliance-Richtlinien.**
- **4. Schutz vor Privilege-Escalation-Angriffen: Schützen Sie sich vor Rechteausweitung in der Cloud mit granularen Einstellmöglichkeiten für die Berechtigung in den einzelnen Datenräumen.**

Das Wichtigste zum Datenaustausch in MS Teams auf einen Blick

Microsoft Teams speichert die Dateien, die Sie hochladen, aber auch zahlreiche Meta-Informationen und personenbezogene Daten. Im Zweifel sind diese Daten vor einem Zugriff nicht geschützt. Im folgenden Abschnitt erfahren Sie die Details rund um das Speichern Ihrer Daten in MS Teams.

Wie bekomme ich Dateien/Dokumente in Teams?
Sie können Dateien per Drag & Drop in Ihr Teams-Fenster ziehen und zwischen den Dateien ablegen. Alternativ können Sie auch die „Hochladen"-Funktion nutzen und dort über „Öffnen aus" die Datei auswählen, die Sie ablegen möchten.

Wie lange bleiben Dateien in Teams gespeichert?
Ein Anrufverlauf unterliegt einer Verfügbarkeitsdauer von 30 Tagen, der Standort des Benutzers und die Standortfreigabe ist 90 Tage verfügbar. Bei Nachrichten, Gruppentiteln, Bildern, im Chat freigegebenen Daten, Kalenderelementen, Benutzerprofilen, Kontakten, Benutzerbeitrittscodes, Gruppenbeitrittscodes, Sicheren Daten, To-dos und Anwesenheitsmeldungen kann der Benutzer selbst bestimmen, wie lange sie verfügbar sein sollen. Diagnosedaten halten bis zu 13 Monaten an, dies kann jedoch der Benutzer in den Datenschutzeinstellungen seines Microsoft-Kontos selbst festlegen.

Wo speichert Teams Aufzeichnungen?
Teams speichert seit 2021 – sofern nicht anders eingestellt – Besprechungsaufzeichnungen auf OneDrive und SharePoint. Zuvor wurden diese Daten in Microsoft Stream gespeichert.

Wo liegen die Teams Hintergrundbilder?
Klicken Sie in Teams einfach– bevor Sie an einer Besprechung teilnehmen– auf die Schaltfläche in der Mitte (zwischen dem Kamera- und dem Mikrofon-Symbol). Nun erscheint rechts eine Auswahl von Bildern, die Sie als Hintergrund verwenden können. Den Hintergrund können Sie übrigens auch während einer Teams-Besprechung verändern. So können Sie z. B. auch Hintergrundeffekte nutzen oder den Hintergrund Ihrer eigenen Umgebung „verwischen". Wenn Sie eigene Hintergrundbilder verwenden möchten, geben Sie den Pfad %APPDATA%\Microsoft\Teams\Backgrounds inklusive der %-Zeichen in Ihren Explorer ein. In dem Ordner „Upload" liegen die bestehenden Hintergrundbilder. Diese können Sie mit ihren eigenen .png- oder .jpg-Dateien ergänzen und diese dann wie vormals beschrieben auswählen. Auf dem Mac rufen Sie einfach das Verzeichnis /Users/UserName/Library/Application Support/Microsoft/Teams/Backgrounds/Uploads auf und hinterlegen dort den gewünschten Hintergrund.

Wie schickt man ein Video in Teams?
Zuerst wählen Sie die Funktion „Stream" aus. Anschließend gehen Sie im Menü auf „Inhalte" und klicken auf „Video hochladen". Sie können die Dateien direkt mit der Maus hinziehen oder über die Funktion „suchen Sie nach Dateien" für den Upload auswählen. Jetzt können Sie festlegen, welche Videodatei Sie verwenden möchten. Im folgenden Fenster können Sie den Namen des Videos ändern und eingeben, die Beschreibung des Inhalts anpassen und eine Miniatur-Vorschau auswählen. Nun haben Sie die Möglichkeit, die Berechtigungen anzupassen und damit festzulegen, welche Personengruppe das Video sehen kann. Wenn Sie abschließend auf „Veröffentlichen" klicken, wird das Video hochgeladen.

Warum tausche ich Daten in MS Teams aus?
Erleichtertes Arbeiten im Homeoffice & einfacher Austausch im klassischen Büroalltag: Mit MS Teams lassen sich Besprechungen, Chats, Notizen und Anhänge digital organisieren und bereitstellen.

Warum muss ich meine Daten DSGVO-konform speichern / teilen?
Die EU-DSGVO gibt genau vor, wie Daten in Deutschland und Europa gespeichert und verarbeitet werden dürfen. Seither gelten noch strengere Regularien, und Verstöße werden mit hohen Bußgeldern sanktioniert.

Warum muss man eine externe Lösung nutzen, um Daten in Teams abzusichern?
Durch den CLOUD Act werden Unternehmen mit Sitz in den USA und Unternehmen, die zu einem US-amerikanischen Mutterkonzern (wie beispielsweise Microsoft) gehören, dazu verpflichtet, für Ermittlungszwecke sämtliche Daten bereitzustellen. In Europa hingegen untersagt die EU-DSGVO eine Herausgabe von personenbezogenen Daten ohne ein gültiges Rechtsabkommen. Das führt zu einem massiven Konflikt.

Warum ist eine Datenspeicherung in MS Teams nicht DSGVO-konform?
Durch den CLOUD Act kollidiert jede Nutzung von MS Teams für ein europäisches Unternehmen mit der EU-DSGVO, sofern dort Daten über die integrierten Dienste gespeichert werden.

Warum ist das ein Problem?
Die US-Regierung stellt durch den CLOUD Act auch den Zugriff auf ausländische Server sicher – dem müssen sich auch europäische Unternehmen beugen, sofern sie ihre Daten nicht anderweitig absichern.

Wie (un)sicher sind Ihre Dateien in MS Teams?

Grundsätzlich besteht bei der Nutzung von MS Teams bzw. Office 365 immer die Gefahr, dass Daten an amerikanische Behörden weitergegeben werden. Begünstigt wird dies durch den Cloud Act. Kombiniert man die Anwendungen aber mit Lösungen zum sicheren Datenaustausch, kann man sich gegen diese Lücke absichern und behält die Hoheit über die eigenen und häufig sensiblen Unternehmensdaten. Neben der Absicherung der ausgetauschten Dateien und Informationen ergeben sich durch den Einsatz einer File Service Plattform wie DRACOON noch weitere Vorteile. Alle Benutzer arbeiten automatisch datenschutzkonform und können die Vorzüge der Microsoft-Produkte nutzen. Die Lösung ermöglich in Outlook die verschlüsselte Zustellung von E-Mail-Anhängen oder bedarfsweise vollends verschlüsselten E-Mails, ohne dass Postfächer physisch belastet werden und das völlig DSGVO-konform. Zudem schützt man sich gleichzeitig vor Ransomware.

In der täglichen Arbeit mit MS Teams oder anderen Office 365-Anwendungen im Büro oder im Homeoffice werden zahlreiche Daten und Dateien ausgetauscht. Das sollte so intuitiv und einfach funktionieren wie nur möglich, ohne dass der Schutz von Daten zu kurz kommt oder zu kompliziert ist. Deshalb bieten sich Filesharing-Lösungen als ideale Ergänzung an.

4. E-MAIL-VERSCHLÜSSELUNG IN OUTLOOK LEICHT GEMACHT

Im täglichen Handling müssen E-Mail-Anhänge beliebiger Größe und komplette E-Mails verschlüsselt bzw. DSGVO-konform versendet werden. Vor allem für Unternehmen wird dies oft zur Herausforderung, denn zum Teil ist der Umgang von Mitarbeitern mit Daten hier problematisch. E-Mail-Anhänge, aber auch Mails können sehr leicht gehackt werden. Die EU-DSGVO regelt hier ganz klar, wie sensible Daten per Mail überhaupt versendet werden dürfen. Darüber hinaus müssen auch KRITIS-Unternehmen besondere Anforderungen erfüllen, wenn sie Daten auf diesem Weg übermitteln möchten.

Klassische E-Mail-Verschlüsselungsprogramme sind sehr umständlich

Viele Unternehmen suchen daher nach einer Lösung, um sensible Dateien trotzdem sicher und DSGVO-konform per E-Mail versenden zu können. Die beiden gängigsten Formen der klassischen E-Mail-Verschlüsselung sind die asymmetrischen Verschlüsselungsverfahren S/MIME (Secure/Multipurpose Internet Mail Extensions) und PGP (Pretty Good Privacy).

Diese Formen der Verschlüsselung von E-Mails benutzen eine asymmetrische Verschlüsselung, bei der zwei Schlüssel zum Einsatz kommen, die zusammenpassen müssen. Zum Verschlüsseln einer Mail wird ein öffentlicher Schlüssel (Public Key) benutzt, der Mail-Empfänger benötigt zum Entschlüsseln den dazugehörigen Private Key. Dieses Verfahren hat den Vorteil, dass nicht nur der Mail-Inhalt an sich verschlüsselt ist, sondern es ist auch gewährleistet, dass der Absender als derjenige authentifiziert ist, der er vorgibt zu sein.

Wenn Sie diese Verfahren in der Praxis verwenden möchten, um Kontakten eine verschlüsselte E-Mail zu schicken, müssen Sie folglich ein Sicherheitszertifikat auf Ihrem Computer installieren und Ihren Kontakten einen sogenannten „Public Key" zukommen lassen. Gleichzeitig muss aber auch der Empfänger ein entsprechendes Zertifikat installiert haben und Ihnen den Public Key zukommen lassen, damit Sie wiederum E-Mails empfangen können. Klassische E-Mail-Verschlüsselungsprogramme, welche diese Verschlüsselungsformen verwenden, sind daher eher umständlich zu bedienen.

Ebenso ist bei der Verwendung einer E-Mail-Verschlüsselung mit OpenPGP und S/MIME der Aufwand für die IT-Abteilung groß: Geltende Zertifikate für diese Form der Verschlüsselung müssen jährlich erneuert werden. Das kostet nicht nur wiederkehrend Geld, sondern auch IT-Ressourcen, weil der Tausch von erfahrenem IT-Fachpersonal durchgeführt werden muss.

Oft ist es jedoch gar nicht nötig, die komplette Mail zu verschlüsseln, da sich die sensiblen Informationen (wie der am Anfang erwähnte Vertrag) im Anhang der Mail befinden. Daher muss sichergestellt werden, dass vor allem der Anhang verschlüsselt zugestellt wird. Trotzdem gibt es auch E-Mails, die höchsten Sicherheitsanforderungen unterliegen – hier ist es notwendig, die vollständige E-Mail verschlüsselt zu versenden.

So versenden Sie E-Mails vollständig verschlüsselt

Mit der E-Mail-Vollverschlüsselung für Outlook gibt es eine hochsichere Versandmethode für besonders sicherheitskritische E-Mails (beispielsweise von DRACOON). Der Begriff „Vollverschlüsselung" bezieht sich auf die Tatsache, dass sowohl die E-Mail-Nachricht selbst als auch etwaige Dateianhänge clientseitig verschlüsselt werden, bevor sie dem Empfänger bereitgestellt werden.

Wenn Sie eine E-Mail vollständig verschlüsselt versenden möchten, wird die E-Mail-Nachricht automatisch in eine clientseitig verschlüsselte PDF-Datei umgewandelt und mitsamt etwaigen Dateianhängen der E-Mail in einen verschlüsselten Datenraum in DRACOON hochgeladen. Die eigentliche E-Mail-Nachricht mit Anhängen wird nicht per Outlook versendet – stattdessen erhält der Empfänger automatisch eine Benachrichtigungsmail mit einem kennwortgeschützten Freigabe-Link, über den er die PDF-Datei mit der E-Mail-Nachricht und die Dateianhänge sicher herunterladen kann. Beim Herunterladen werden diese durch Eingabe des Kennworts entschlüsselt und können vom Empfänger geöffnet werden.

Auch wenn die internen Abläufe der E-Mail-Vollverschlüsselung komplex sind, so ist die Verwendung für Absender und Empfänger dennoch einfach und komfortabel. Denn verglichen mit dem regulären E-Mail-Versand ist nur ein zusätzlicher Schritt notwendig: Der Absender muss lediglich ein Kennwort für die E-Mail angeben bzw. erzeugen lassen und dieses dem Empfänger manuell zusenden (z.B. per Chat), damit dieser die E-Mail entschlüsseln und öffnen kann.

Daher beinhaltet DRACOON für jeden Benutzer – neben dem sicheren Speicherort für alle Daten – gleichzeitig eine DSGVO-konforme Lösung zur E-Mail-Verschlüsselung. So kommunizieren Sie einfach und sicher per E-Mail – und haben gleichzeitig die volle Kontrolle über Ihre Dateien.

Vorteile der E-Mail-Vollverschlüsselung

Inhalt und Anhänge einer durch DRACOON für Outlook vollverschlüsselten E-Mail werden nicht über Ihren regulären Mailserver versendet und können daher auf dem Versandweg und durch Server-Administratoren nicht abgegriffen werden.
Sie werden außerdem nicht im Postfach des Empfängers gespeichert, sodass auch auf Empfängerseite kein Datenabfluss z.B. durch Server-Administratoren möglich ist.
Die clientseitige Verschlüsselung stellt sicher, dass Inhalt und Anhänge der Mail bereits auf dem PC des Absenders sicher verschlüsselt werden, bevor Sie in DRACOON hochgeladen werden – durch die clientseitige Verschlüsselung wäre z.B. selbst DRACOON als Anbieter in keinem Fall in der Lage, die E-Mail zu entschlüsseln.
Durch ein Ablaufdatum kann die Verfügbarkeit der E-Mail zeitlich begrenzt werden, sodass Sie danach vom Empfänger nicht mehr heruntergeladen und geöffnet werden kann. Im Bedarfsfall kann die Bereitstellung der E-Mail durch Löschen des Freigabe-Links auch jederzeit vorzeitig beendet werden.
Absender und Empfänger müssen keine Zertifikate austauschen, wie es bei der in Outlook enthaltenen Mail-Verschlüsselung (per S/MIME) erforderlich ist. Der Absender muss dem Empfänger lediglich ein Kennwort mitteilen.

5. GIBT ES MÖGLICHKEITEN, DIE VORTEILE VON MICROSOFT 365 ZU NUTZEN, OHNE EINEN DSGVO-VERSTOSS ZU BEGEHEN?

Beim Einsatz der Microsoft 365 Produkte sollte man verschiedene Aspekte des Datenschutzes genauer betrachten. Die Lösung datenschutzkonform / GDPR-konform einzusetzen kann eine Herausforderung für Unternehmen sein, besonders wenn sie besonderen Regularien unterliegen wie: DSGVO, HIPAA, CCPA, TISAX, FINRA oder ITAR.

Die Produkte der Firma DRACOON verfolgen einen sehr interessanten Ansatz. DRACOON hat Plug-ins entwickelt, die die Vorteile von OneDrive und der Microsoft 365-Produktpalette verfügbar machen und trotzdem die GDPR einhalten. Dazu werden die Daten ausschließlich auf den DRACOON-Servern gespeichert und die Verarbeitung der Daten findet nur lokal auf den Arbeitsplatzrechnern statt. Damit soll sichergestellt werden, dass Microsoft zu keinem Zeitpunkt Zugriff auf die Daten hat.

Nicht erst seit COVID-19 sind die Microsoft Programme zu unverzichtbaren Wegbegleitern des digitalen Arbeitens geworden. Der Schritt in die Microsoft Cloud führt jedoch zwangsläufig zu einem Kontrollverlust, den man aber mit der richtigen Lösung vermeiden kann.

6. EXKURS DATENSCHUTZ

Unter dem Begriff „Datenschutz" versteht man den Schutz vor einer missbräuchlichen Verarbeitung von personenbezogenen Daten und den Schutz des Rechts auf eine informationelle Selbstbestimmung: Jeder einzelne kann grundsätzlich darüber entscheiden, welche personenbezogenen Daten er preisgibt und ob sie verwendet werden dürfen.
Ein Schutz von personenbezogenen Daten ist dann erforderlich, wenn verantwortliche Stellen gemäß der Datenschutzgrundverordnung personenbezogene Daten verarbeiten. Beim Datenschutz geht es generell darum, Informationen zu schützen, die nicht für die Allgemeinheit gedacht sind. Personenbezogene Daten sind insbesondere private und persönliche Daten, die Rückschlüsse auf eine Person zulassen. Es handelt sich also vor allem um Kontaktdaten wie den Namen, Telefonnummer, Anschrift, E-Mail-Adresse, Geburtsdatum, aber auch die IP-Adresse.

Unter Datenschutz versteht man also den Schutz des Persönlichkeitsrechts nach Artikel 1 und 2 des Grundgesetzes bei der Verarbeitung von Daten und den Schutz der eigenen Privatsphäre des Menschen. Verstöße gegen den Datenschutz werden mit Bußgeldern von bis zu 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes der verantwortlichen Stelle bestraft. Auch eine Freiheitsstrafe von bis zu 3 Jahren ist möglich.

Warum ist Datenschutz wichtig?

Mit Hilfe des Datenschutzes lassen sich personenbezogene Daten vor einem Datenmissbrauch schützen. Gerade im Zusammenhang mit der fortschreitenden Digitalisierung spielt ein derartiger Schutz eine immer größere Rolle.

So wurden beispielsweise Daten der Teilnehmer eines Gewinnspiels der Krankenkasse AOK für Werbezwecke eingesetzt, obwohl diese einer Verwendung für Marketingmaßnahmen nicht zugestimmt hatten. Die Krankenkasse hatte zwar versucht, durch technische und organisatorische Maßnahmen sicher zu stellen, dass ausschließlich Personen kontaktiert werden, die ihre Zustimmung erteilt hatten, aber diese Maßnahmen erwiesen sich nach den gesetzlichen Vorgaben als unzureichend. Die zuständige Landesbehörde verhängte daraufhin ein Bußgeld von 1,24 Millionen Euro.

Für Betroffene kann es auch schwerwiegende Folgen haben, wenn z. B. die private E-Mail-Adresse bekannt wird und schützenswerte Details über die eigene Krankheitsgeschichte oder Chatverläufe von privaten Gesprächen öffentlich zugänglich gemacht werden. Gleiches gilt natürlich auch für sensible Bankdaten. Im Zuge der Digitalisierung hat der Datenschutz enorm an Bedeutung gewonnen, gerade weil beispielsweise auch durch das Surfverhalten zahlreiche Daten und somit Informationen über das Nutzerverhalten von Dritten gesammelt werden können.

Wer prüft den Datenschutz?

Die Einhaltung des Datenschutzes wird durch die jeweils zuständige Aufsichtsbehörde überwacht. Für Unternehmen bedeutet das, dass die jeweiligen Beauftragten für den Datenschutz der Länder diese Aufgabe übernehmen. Zudem soll der Datenschutzbeauftragte als unabhängige Instanz im Unternehmen auf die Einhaltung

der Regularien hinwirken. Damit übernimmt er quasi auch eine Kontrollfunktion, die eigentlich auch den Aufsichtsbehörden obliegen würde. Datenschutzverstöße werden mittlerweile ebenfalls dem Verbraucherschutz zugeordnet, u. a. deswegen, weil sie auch eine rechtliche Relevanz haben. Daher können Verstöße auch durch die Verbraucherschutzorganisationen oder etwaige Mitbewerber durch Abmahnungen geahndet werden.

Generell ist Datenschutz jedoch Chefsache, das bedeutet, das sich auch der Geschäftsführer einer GmbH darum kümmern muss, dass der Datenschutz eingehalten wird. Seit Inkrafttreten der EU-DSGVO haftet dieser auch erst einmal für die vermeintlichen Fehler seiner Mitarbeiter. Im Zuge dessen ist der Verantwortliche auch in der Beweislast bzw. der Nachweispflicht, dass er alle Regeln befolgt hat. Um eine unabhängige Beurteilung zu erhalten, können sich Unternehmen einem sogenannten Datenschutzaudit unterziehen. Passende Auditoren werden beispielsweise über den Bundesverband der Datenschutzbeauftragten Deutschlands (BvD) und der Gesellschaft für Datenschutz und Datensicherheit (GDD) vermittelt.

Wie ist der Datenschutz in Deutschland geregelt?

In Deutschland gilt wie oben beschrieben die Datenschutzgrundverordnung. Hergeleitet wird das Datenschutzrecht aus dem Recht auf informationelle Selbstbestimmung. Darin ist festgelegt, dass jeder grundsätzlich selbst entscheiden kann, wie mit seinen personenbezogenen Daten umgegangen werden soll. Der Begriff der „personenbezogenen Daten" spielt im Datenschutzrecht eine zentrale Rolle. Denn nur dann, wenn Daten einen Bezug zu einem Menschen aufweisen (also z. B. bei Namen, Geburtstag, Adresse, E-Mail-Adresse, IP-Adresse oder der Bankverbindung), kommt das Datenschutzrecht zur Anwendung.

Zu den wichtigsten Grundsätzen des Datenschutzrechts gehören:

- **Verbot mit Erlaubnisvorbehalt**
  Ein Umgang mit Daten darf nur dann erfolgen, wenn es dazu eine gesetzliche Grundlage gibt oder der Betroffene zugestimmt hat.

- **Rechtmäßige Verarbeitung nach Treu und Glauben, Transparenz**
  Die Datenverarbeitung muss auf rechtmäßiger Weise, nach dem Grundsatz von Treu und Glauben und in eine für die betroffene Person nachvollziehbare Weise erfolgen.

- **Zweckbindung**
  Daten, die für einen bestimmten Zweck erhobenen bzw. gespeicherten Daten wurden, dürfen auch nur für diesen Zweck verwendet werden.

- **Datenminimierung**
  Nach dem Grundsatz der Datenminimierung müssen die personenbezogenen Daten dem Zweck angemessen und für diesen erheblich sein. Die Daten sind auf das notwendige Maß zu beschränken, das für die Verarbeitung notwendig ist.

- **Speicherbegrenzung**
  Ist der verfolgte Zweck erreicht ist, müssen die Daten gelöscht werden.

- **Richtigkeit der Daten**
  Die erhobenen und verarbeiteten Daten müssen sachlich richtig und auf dem neuesten Stand sein.

- **Integrität und Vertraulichkeit**
  Personenbezogene Daten müssen mit geeigneten technischen und organisatorischen Maßnahmen in einer Weise verarbeitet werden, die eine Identifikation der betroffenen Person nur so lange ermöglicht, wie es für den Zweck der Datenbearbeitung erforderlich ist.

- **Rechenschaftspflicht**
  Der im datenschutzrechtlichen Sinne Verantwortliche muss die Einhaltung der oben genannten Grundsätze nachweisen können.

Wie können Sie Ihre Daten schützen?

- **Datenschutz bei Cloud-Anbietern - verwenden Sie für die Speicherung und Verwaltung Ihrer Daten einen zertifizierten File Service**
  Es ist essentiell, dass auch Ihr Cloud-Anbieter Datenschutz als wichtiges Thema sieht. Achten Sie darauf, dass Sie Ihre Daten unter maximalen Sicherheitsvorkehrungen speichern können. Ideal ist hier ein cloudbasierter Datenspeicher eines zertifizierten Anbieters, der über eine clientseitige Verschlüsselung verfügt. So haben Sie an jedem Ort gesichert Ihre persönlichen Daten zur Verfügung. Nur so können Sie auch beim Datenschutz in der Cloud der DSGVO gerecht werden.

- **Medizinische Daten und Datenschutz**
  Gerade bei Daten aus dem Gesundheitswesen spielt der Datenschutz eine große Rolle. Vor allem wenn personenbezogene Daten, die zudem auch noch Informationen zu Erkrankungen und aktuellen Befunden umfassen, ist höchste Vorsicht geboten. Wenn Untersuchungsergebnisse, Laborberichte oder umfangreiche Gesundheitsdaten in falsche Hände gelangen, ist der Schaden immens. Moderne und zertifizierte Enterprise File Services liefern jedoch die Basis dafür um dennoch Daten sicher und in Echtzeit an den Stellen, an denen sie benötigt werden, bereitzustellen.

- **Setzen Sie auf verschlüsselte Download-Freigaben**
  Der Versand von ungesicherten Dateianhängen kann großen Schaden anrichten. Nicht selten werden gerade E-Mail-Anhänge gehackt und so geraten sensible Daten in falsche Hände. Auch die EU-Datenschutzgrundverordnung (DSGVO) verbietet es inzwischen, personenbezogene Daten per Mail-Anhang zu versenden. Über ein Add-In zur E-Mail-Verschlüsselung können Sie verschlüsselte Download-Freigaben erstellen. Zudem können Sie alle Dateien in ihrer Verfügbarkeit begrenzen oder aber auch zusätzlich mit einem gesonderten Passwort absichern.

- **Geben Sie so wenig an persönlichen Daten wie möglich preis**
  Überlegen Sie sich genau, welche Informationen sie angeben möchten.

- **Lesen Sie immer die Datenschutzbestimmungen**
  Generell ist jeder an die Datenschutzgesetze gebunden. Achten Sie darauf, welche Daten zu welchem Zweck erhoben, verarbeitet und gespeichert werden.

- **Achten Sie auf die Vertrauenswürdigkeit des Anbieters und eine sichere Verschlüsselung**
  Geben Sie persönliche Daten nur auf vertrauenswürdigen Websites ein, die über eine sichere https-Verbindung verfügen.

Verwenden Sie sichere Passwörter
Ein sicheres Passwort besteht aus einer Kombination von Buchstaben (Groß- und Kleinschreibung) sowie Sonderzeichen und Zahlen. Achten Sie darauf, dass Sie jedes Passwort nur einmal verwenden und halten Sie dieses Passwort geheim. Hilfreich sind auch spezielle Programme, mit den Sie sichere Passwörter generieren oder verwalten können.

Optimieren Sie die Sicherheitseinstellungen Ihres Browsers
In Ihrem Internetbrowser können Sie weitere Einstellungen zur Wahrung Ihrer Daten vornehmen. Überprüfen Sie diese regelmäßig und achten Sie auch hier auf eine maximale Sicherheit durch regelmäßige Updates.

Schützen Sie Ihre Geräte
Ihre verwendeten Geräte können Sie dadurch schützen, indem Sie eine geeignete Sicherheitssoftware installieren, diese auf dem neuesten Stand halten und nur gesicherte (verschlüsselte) W-LAN-Verbindungen nutzen. Verwenden Sie auf Ihrem Computer eine geeignete Antiviren-Software und achten Sie auf eine Firewall.

Vorsicht bei der Nutzung öffentlicher Computer
Seien Sie besonders vorsichtig, wenn Sie öffentliche Computer z. B. in der Schule oder in einem Internetcafé nutzen. Verwenden Sie an diesen Geräten am besten keine allzu sensiblen Daten (wie z. B. Bankdaten). Wenn Sie sich hier auf einer Website einloggen, denken Sie unbedingt daran, dass Sie sich auch zum Schluss wieder ausloggen. Nutzen Sie verschlüsselte Seiten.

Ignorieren Sie Spam-E-Mails
Beantworten Sie weder Fragen noch teilen Sie mit, dass Sie künftig keine E-Mails mehr von diesem Absender möchten. Damit würden Sie nämlich nur bestätigen, dass es sich bei Ihrer Mailadresse um eine gültige E-Mail handelt – und umso mehr Spam bekommen Sie später.

Vermeiden Sie einen Datenklau durch Phising-E-Mails
Geben Sie keine Bank- oder sonstige Zugangsdaten im Internet oder per Mail weiter. Wenn Sie unsicher sind, kontaktieren Sie Ihre Hausbank. Prüfen Sie regelmäßig Ihre Kontoauszüge auf inkorrekte Abbuchungen. Durchschnittlich braucht es 37 Tage, bis ein Datenmissbrauch entdeckt wird.

Öffnen Sie nicht alle Attachments
Klicken Sie keine unbekannten Dateianhänge aus E-Mails an – sie könnten Spyware, die persönliche Daten auf Ihrem Computer ausspioniert oder Viren enthalten.

Hinterfragen Sie Ihr Online-Verhalten
Seien Sie sich darüber im Klaren, dass alle Daten, die Sie im Internet stellen, für gewöhnlich weltweit zugänglich und über Suchmaschinen auffindbar sind.

Prüfen Sie die Privatsphäre-Einstellungen in sozialen Netzwerken
Über die Privatsphäre-Einstellungen von Anwendungen können Sie festlegen, wer welche Informationen von Ihnen einsehen kann und wer sie weiterverarbeiten darf. So können Sie beispielsweise einschränken, dass nur tatsächliche Freunde alle Beiträge sehen können.

Werden Sie bei Verstößen gegen den Datenschutz aktiv
Nehmen Sie ggf. mit der Landesdatenschutzbehörde oder der Verbraucherschutzzentrale https://www.verbraucherzentrale.de/beschwerde auf. Wenn Daten gestohlen werden, ist dies außerdem ein Fall für die Polizei.

Nutzen Sie Nicknames
Verwenden Sie – wenn möglich – anonyme Nicknames anstelle Ihres richtigen Namens. In sozialen Netzwerken könnten Sie beispielsweise auch Ihren Zweitnamen verwenden.

Verwenden Sie mehrere E-Mail-Adressen
Legen Sie sich bei einem Gratis-Anbieter eine E-Mail-Adresse an, die keine Rückschlüsse auf Ihre Person zulässt. Verwenden Sie diese Adresse, um sich auf Websites zu registrieren, in Blogs zu posten oder in Foren mitzudiskutieren.

Löschen Sie Ihre persönlichen Daten
Achten Sie darauf, dass Sie sämtliche persönlichen Daten löschen, bevor Sie ein Gerät (Smartphone, Tablet oder PC) verkaufen.

Augen auf bei der Installation von Apps
Prüfen Sie vor der Installation einer App, für welche Daten Sie den Zugriff autorisieren. Manchmal versteckt sich gerade im Kleingedruckten die wichtigste Information.

Galgenbergstrasse 2a • 93053 Regensburg
+49 941 - 78385-0 • info@dracoon.com