netmail

Compliance Anforderungen und Office 365

Exchange Online, Office 365 und die gesetzlichen Anforderungen an Aufbewahrung (GoBD), Auskunftsfähigkeit und das Recht auf Vergessen (DSGVO)

Key Facts

Eine vollständige Abdeckung, der in Deutschland gängigen Anforderungen an Compliance, ist mit den Standard Möglichkeiten in Office 365 im Rahmen des E3 Plans oder Exchange Online 2 Plans, nahezu unmöglich und in der Praxis nicht nutzbar. Gerade bei erlaubter oder geduldeter Privatnutzung oder einem gemischten Betrieb zwischen On-Premise und Cloud nicht abbildbar.

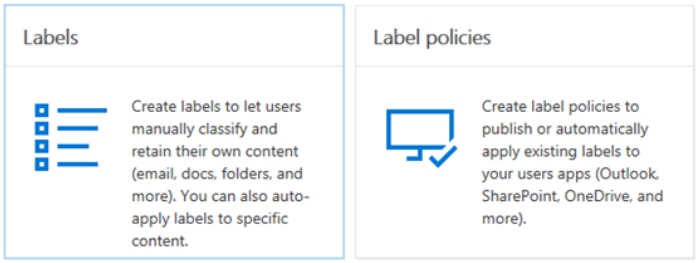
Erst mit dem Advanced Compliance Modul (Bestandteil E5 oder dediziert für 6,70 € / Monat / User zzgl. MWSt. zubuchbar) ist ein vollständiges E-Discovery nach EDRM möglich, wenngleich limitiert auf Office 365.

Vorstellung der Compliance Module in Office 365

O365 bietet mittlerweile eine Reihe von neuen Funktionen im Rahmen der „Security & Compliance“ Komponenten. Diese sind in der Basis Variante Bestandteil des E3 Plans oder des Business Essentials für kleinere Unternehmen.

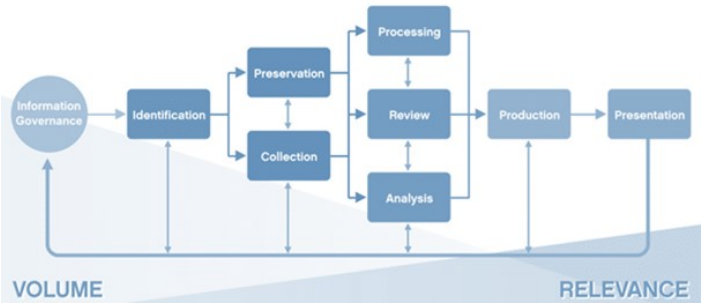
Das Security & Compliance Portal bietet im Grundsatz die Möglichkeit, innerhalb der Office 365 Produkte, Daten und Informationen zu durchsuchen und zu verwalten. Unternehmen können z.B. E-Discovery Fälle bei Rechtsstreitigkeiten erstellen und somit Daten über Teams, Skype, OneDrive, Sharepoint und Exchange durchsuchen. Hierbei können alle Office 365 Quellen und Accounts inspiziert oder selektiv ausgewählt werden. Auch eine Ablaufhemmung, z.B. bei laufenden Steuerprüfungen zurückliegender Jahre, ist einfach zu erstellen. Dies geschieht im E-Discovery-Fall über sogenannte „Holds“, Litigation Hold oder Retention Policies.

Nicht zuletzt durch die Anforderungen der DSGVO bekommt die Kategorisierung von unstrukturierten Daten, wie E-Mails, Dateien und sonstigen durch den Anwender erstellten Inhalten, eine immer größere Bedeutung. Hier arbeitet Microsoft in Office 365 mit sogenannten „Labels“. Diese können im „Data Governance-Retention“ Bereich selbst erstellt, oder aus Vorlagen ausgewählt werden. Die Vorlage für personenbezogene Daten in Deutschland sind allerdings auf Personalausweisnummer und Führerscheinnummer limitiert und sorgen daher für keinen ersichtlichen Mehrwert.



Labels können automatisch zugewiesen oder für den Anwender zur Verfügung gestellt werden. An unterschiedliche Labels können dann Aufbewahrungsrichtlinien verankert werden.

Eine Künstliche Intelligenz (Machine Learning) zur automatischen Klassifizierung und weitere in der Praxis notwendige Funktionalitäten, wie Analyse und Review der E-Discovery Vorgänge sowie Suchergebnisse, ist dem Advanced Compliance Modul vorbehalten. Dieses ist Bestandteil des E5 Plans oder für E3 und Business Essentials separat zubuchbar (6,70 € / Monat / User zzgl. MWSt.). Nur unter Nutzung dieses Moduls ist ein vollständiges E-Discovery gemäß EDRM (Electronic Discovery Reference Model) möglich.



Zusammengefasst ist das neue Compliance Modul eine Weiterentwicklung der eher rudimentären E-Discovery Möglichkeiten in der Vergangenheit. Die Möglichkeiten im Rahmen der Basis Compliance lassen die Aufbewahrung, die Suche und den Export der Suchergebnisse zu. Größere mittelständische Unternehmen und alle Unternehmen, die nicht alle unstrukturierten Daten ausschließlich in Office 365 haben, werden mit dem Basis Compliance Modul nicht auskommen.

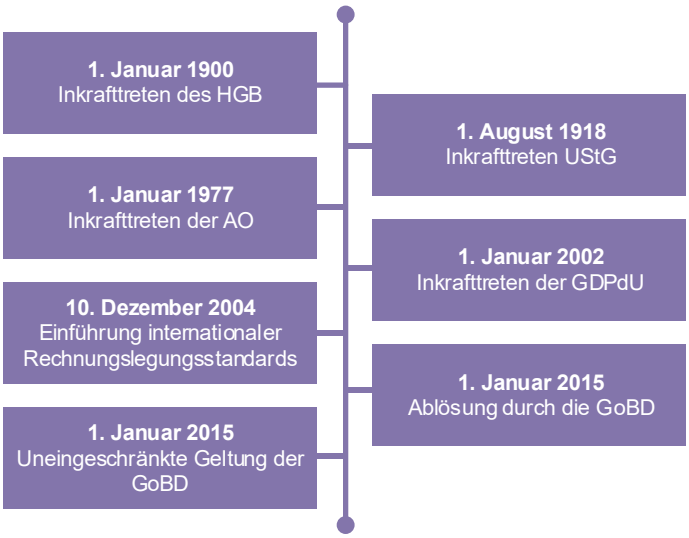
netmail

In der Praxis sind Multi Cloud/Hersteller Strategien und hybrider Betrieb (z.B. das Dateisystem weiterhin On-Premise) weit verbreitet und derzeit im zentraleuropäischen Raum Standard. Das Office 365 Compliance Modul bezieht sich lediglich auf Dienste in Office 365.

Gesetzliche Anforderungen an E-Mail sowie an unstrukturierte Daten

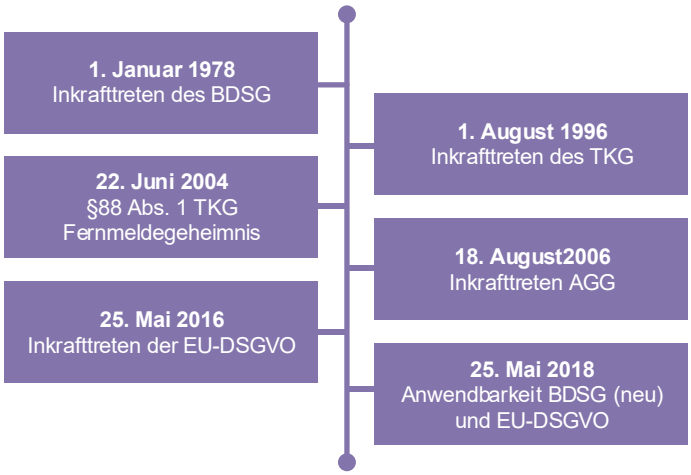
Es gibt eine Reihe von gesetzlichen Anforderungen, die Unternehmen für eine gesetzeskonforme Aufbewahrung zu erfüllen haben. Nicht erst seit Inkrafttreten der DSGVO konkurrieren hierbei eine geforderte revisionssichere Aufbewahrung mit dem Umgang mit privaten bzw. personenbezogenen Daten und somit dem Datenschutz. In der Folge sind die wichtigsten gesetzlichen Anforderungen zusammengefasst.

GoBD: Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) regeln u. a. die Aufbewahrung von geschäftsrelevanten E-Mails. Dabei werden innerhalb des Schreibens unterschiedliche Gesetze aufgegriffen. Insbesondere nachfolgende Gesetze und Verordnungen sind dabei für die E-Mail-Archivierung von Relevanz:



Die Archivierung von E-Mails ist ein umstrittenes Thema, vor allem, wenn es darum geht, geschäftsrelevante E-Mails von den „anderen“ E-Mails zu unterscheiden. Um geschäftsrelevante E-Mails vollständig und lückenlos zu archivieren und um zu vermeiden, dass Daten, ob beabsichtigt oder aus Versehen, verloren gehen, entscheiden sich die meisten Unternehmen dazu, alle Daten des E-Mail-Systems zu archivieren.

Mit einer GoBD-konformen Archivierung ist jedoch keine vollständige Gesetzeskonformität hergestellt, denn einige Gesetze werden in den GoBD nicht behandelt. Daher gilt es bei der E-Mail-Archivierung und insbesondere bei der konkreten Entscheidung für eine Archivlösung weitere Aspekte zu berücksichtigen. Um eine vollumfängliche Gesetzeskonformität herzustellen, müssen alle relevanten Gesetze beachtet werden. Hierunter fallen insbesondere die europäische Datenschutzgrundverordnung (EU-DSGVO/DSGVO), das Telekommunikationsgesetz (TKG) und das Allgemeine Gleichbehandlungsgesetz (AGG), die von einer Archivlösung Flexibilität fordern.



BDSG und DSGVO: Das BDSG sowie die DSGVO ermöglichen es natürlichen Personen (sogenannten “Betroffenen”) Auskünfte über deren personenbezogene Daten zu verlangen. Die Auskünfte sind binnen eines Monats zur Verfügung zu stellen. Auch entsprechende Archivdaten müssen auffindbar sein und bereitgestellt bzw. exportiert werden. Eine Löschung muss möglich sein, sofern die Daten keine geschäftsrelevanten Inhalte aufzeigen. Gerade diese Möglichkeit wird von einigen Systemen nicht vollumfänglich unterstützt.

Ablaufhemmung gemäß Abgabenordnung (AO): Geschäftsrelevante Daten werden mitunter über eine Dauer von 10 Jahren gespeichert. Doch auch eine frühzeitige Löschung ist umzusetzen, sofern die Daten nicht geschäftsrelevant sind und gelöscht werden können. Mit der Ablaufhemmung werden bestimmte Daten aus der automatischen Löschung genommen und somit „vom Ablauf gehemmt“. Diese Flexibilität ist insbesondere bei laufenden Prüfungen oder Rechtstreitigkeiten von Bedeutung für viele Unternehmen.

Private Kommunikation nach TKG: Die gesonderte Handhabung von sensiblen und insbesondere privaten Daten ist eine weitere wichtige Komponente. Viele Unternehmen sind der Meinung, dass ein Verbot der Privatnutzung, z.B. durch eine Betriebsvereinbarung, ausreichend ist. Für die Umsetzung des Verbots ist allerdings eine regelmäßige stichprobenartige Überprüfung erforderlich. Anderenfalls kann der Arbeitnehmer für die Privatnutzung des E-Mail-Kontos einen Anspruch nach den Grundsätzen betrieblicher Übung erwerben (Gewohnheitsrecht) und das Verbot geht automatisch in eine Duldung über. Solche Daten sind gesondert und besonders geschützt aufzubewahren.

Der Zugriff auf diese Daten ist, z.B. durch Mehraugenprinzip und getrennte Datenbereiche, besonders zu schützen.

Zusammenfassung der gesetzlichen Anforderungen

Zusammenfassend gibt es eine Menge von gesetzlichen Vorgaben, die zu beachten sind. Je nach Branche kommen weitere Auflagen hinzu. Manche Vorgaben stehen durchaus im Konflikt mit anderen und hier ist meist die geschäftsrelevante Vorgabe höher zu bewerten. Ein besonders wichtiger Punkt beim Umgang mit Daten ist die Möglichkeit der Klassifizierung und unterschiedlicher Behandlung bzw. Speicherung (Privat, personenbezogene Daten, Bewerbungen, Betriebsrat, sensible Informationen, „normale“ geschäftliche Daten).

Im Falle der Privatnutzung, z.B. des E-Mail-Systems, was in 90% der Unternehmen zumindest im Rahmen der Duldung der Fall ist, muss der Anwender die Möglichkeit haben, diese zu kennzeichnen und dadurch in den Systemen unter besonderen Schutz zu stellen. Unzulässig gespeicherte Daten müssen gelöscht werden können. Auch bei abgelehnten Bewerbungen hat der Bewerber das Recht auf vollständige Löschung, genauso wie bei personenbezogenen Daten, die für den tatsächlich geschäftlichen Kontext nicht mehr relevant sind. Es gibt also in der Praxis eine Vielzahl an Fällen, in den Nachrichten und Daten gelöscht werden müssen (auch aus Archiven).

Problematik

Bei der Umsetzung der gesetzlichen Anforderungen ausschließlich mit Office 365 Modulen gibt es eine Reihe von Herausforderungen, die auf den ersten Blick oft nicht ersichtlich sind. Mit Fokus auf die E-Mail-Kommunikation wird dies schnell klar. Die größte Hürde stellt hierbei die lückenlose, revisionssichere Aufbewahrung (Archivierung) von gesetzlich/steuerlich relevanten E-Mails und eine gleichzeitige Privatnutzung oder Duldung des Systems dar.

Hierfür zuerst eine Ausführung zu dem Exchange Online Archiv, welches Bestandteil des Exchange Online Plan 2 oder Office E3 Plans ist: Das Exchange Online Archiv ist kein E-Mail -Archiv im Sinne von Compliance. Auch wenn der Name anderes vermuten lässt, ist das Online Archiv Postfach lediglich ein weiteres Postfach, in welches der Anwender Nachrichten verschieben kann, oder per MRM auf Systemordner Regeln gesetzt werden können. Mit nahezu unlimitiertem Speicherplatz können im Archiv Postfach im Grunde lebenslang Daten aufbewahrt werden. Dies obliegt im ersten Schritt aber dem Anwender selbst, es sei denn es wird systemseitig auf Litigation Hold gesetzt bzw. mit einer Retention Policy belegt. Dann werden allerdings ALLE Daten, auch personenbezogene Daten, ohne Ausnahme aufbewahrt. Diese Option ist auch erst mit dem E2 Plan verfügbar. Compliance Themen werden über die Compliance Module in Verbindung mit E-Discovery, Retention Policies, Labels und weiteren durchgeführt.

Für eine gesetzeskonforme Compliance-Archivierung bedarf es jedoch großer Flexibilität und granularer Einstellmöglichkeiten bei der Kategorisierung der Daten und vor allem beim Zugriff (Suche & Prüfung) auf die E-Mail Nachrichten. Die Aufbewahrung von geschäftlichen Nachrichten und personenbezogenen Daten im gleichen System und gleichen Zugriffsmöglichkeiten ist problematisch. Personenbezogene und private Daten müssen vor unerlaubten Zugriff geschützt sein. Vor allem jedoch bei der Anforderung einer Löschung von ungerechtfertigt gespeicherten Daten (z.B. personenbezogenen Daten oder abgelehnter Bewerbungen) müssen sehr häufig selektive Löschungen von Nachrichten durchgeführt werden.

Um nicht die Anforderungen seitens GoBD an die Aufbewahrung der E-Mails zu unterlaufen, muss der Prozess protokolliert und in Zustimmung von z.B. der internen Revision & Rechtsabteilung oder Datenschützer durchgeführt werden. Eine Löschung von Daten im Exchange System lässt sich, wenn überhaupt, nur mit erheblichem Aufwand durchführen und ist keinesfalls für viele Mailboxen praktikabel durchführbar. Die Problematik liegt an der Arbeitsweise des sogenannten „Dumpster“ oder „Recoverable Items“-Bereiches im Exchange (Online). Dieser hält Nachrichten bei Setzen von Litigation Hold oder Retention Policies vor und verhindert ein Löschen von Nachrichten. Dies ist notwendig, um lückenlos und revisionssicher Nachrichten vorhalten zu können. Die Anforderungen seitens DSGVO beschreiben jedoch ein Recht auf Vergessen und hierdurch entstehen eine Menge an Prüfungsvorgängen.

Auch seitens der Unternehmen gibt es Gründe nicht benötigte und gewünschte Nachrichten, wie z.B. Phishing E-Mails oder Nachrichten mit Malware im Anhang, die am Gateway nicht erkannt wurden, aus den Postfächern zu löschen. Wenn nun Litigation Hold temporär von der Mailbox genommen wird oder die Retention Policy weggenommen wird, dürfen allerdings Nachrichten (z.B. abgelaufene Nachrichten) aus diesem Bereich unkontrolliert das System verlassen.

Was tun? Warum machen ergänzende Lösungen für Office 365 Sinn?

Office 365 ist eine umfassende und gute Cloud-Lösung für Basis Infrastruktur Applikationen. Jedoch wird es immer Spezialanbieter und Lösungen geben, die sich auf bestimmte Problematiken und Herausforderungen fokussieren und letztlich bessere und notwendige Lösungen bieten. Ein Multifunktionsdrucker kann prinzipiell auch Drucken & Scannen und reicht für viele Privatanwender völlig aus.

Trotzdem gibt es dedizierte Drucker und dedizierte Scanner, die in Unternehmen für umfassendere Anforderungen nicht wegzudenken sind. Auch bei DSGVO, Exchange Online und der Datenhaltung in Office 365 gibt es jede Menge Gründe für (Cloud) Lösungen von Drittanbietern wie Netmail.

Vollständiges E-Discovery, auch bei Multi Cloud/Hersteller Strategien und hybriden Umgebungen

Multi Cloud oder hybride Umgebungen sind weit verbreitet. Sharepoint und Exchange sind unter Umständen in Office 365 oder im hybriden Modus, das Dateisystem mit klassischen Home- und Gruppenlaufwerken oft On-Premise, oder von einem anderen Softwarehersteller. Die Compliance Anforderungen unterscheiden jedoch nicht zwischen Cloud und On-Premise. Es ist eine ganzheitliche Lösung zu schaffen. Dies ist mit den Office 365 Compliance Modulen nicht möglich.

Drittanbieter, wie Netmail, bieten ganzheitliche Lösungen für einen Mischbetrieb mit einem professionellen E-Discovery Framework und Workflows an. Dies umfasst rollenbasierte Zugriffsmöglichkeiten für die Aufbereitung und Analyse der Daten gemäß E-Discovery Reference Model (EDRM) und geht weit über die Basisfunktionalitäten von Office 365 hinaus.

Zugriffsschutz für personenbezogene Daten durch Mehraugenprinzip, getrennte Speicherung der geschäftlichen Daten von personenbezogenen, sensiblen und privaten Daten entsprechen den gesetzlichen Anforderungen, sind jedoch mit Office 365 alleine nicht zu realisieren. Eine automatische Klassifizierung von Daten mit Hilfe von KI (Künstlicher Intelligenz) sind ebenso Bestandteil wie zentral einstellbare Richtlinien. Auch können bestehende Labels und Klassifizierungen, die durch die Office 365 Basis Compliance gesetzt worden sind, verwertet werden. Dies nicht nur für Office 365, sondern auch viele weitere Applikationen für unstrukturierte Datenspeicherung, wie Dropbox, Box, Citrix ShareFile, Egnyte, Windows Dateisystem und viele mehr.

Ein gemeinsames, rollenbasiertes Arbeiten an einem Prüfungsvorgang oder E-Discovery Fall, durch Anwälte, Auditoren, Datenschutzbeauftragten und Reviewer über alle Datenquellen hinweg, ist komfortabel möglich. Die bearbeiteten und selektierten Ergebnisse können letztlich in verschiedenste Standard-Formate übergeben und exportiert werden.

Sollten in einem Unternehmen somit unstrukturierte Daten außerhalb von Office 365 gespeichert werden – was in den meisten Unternehmen der Fall sein wird – so benötigt man hierzu eine professionelle E-Discovery-Applikation, die dies unterstützt. Es ist also keinesfalls eine Entweder-oder-Frage, sondern eine notwendige Erweiterung der Compliance Module in Office 365, funktionell und hinsichtlich der verschiedenen Datenquellen.

Zusätzliches Backup

Ein rechtssicheres Backup als Verpflichtung der IT-Compliance sowie Kontinuitätsmanagement für kritische Applikationen, wozu in den allermeisten Fällen auch E-Mail gehört, ist ein zwingender Bestandteil des Risikomanagements. Dies beinhaltet das schnelle Wiederanlaufen nach einem Ausfall oder Datenverlust. Datenverlust bedeutet dabei nicht zwingend den Ausfall des gesamten Systems.

Auch zu On-Premise Zeiten war nicht nur der vollständige Katastrophenfall, verbunden mit einem totalen Datenverlust, der einzige Grund einer Datensicherung. Viel häufiger wurden Wiederherstellungen von einzelnen Dateien oder E-Mail-Postfächern, Nachrichten und Ordnern durchgeführt.

Dies können Sie z.B. mit einem Cloud-Archivsystem erreichen. Sie haben die Daten in einem unabhängigen, zweiten System gespeichert und können damit einen Notfall-/Wiederanlaufplan unabhängig von Office 365 beschreiben. Versehentlich gelöschte oder zerstörte Daten aus Postfächern können selektiv, auch nach mehr als 30 Tagen, zurückgespielt werden.

Einfache Möglichkeiten der Löschung

Wie beschrieben, sind Löschanfragen bei Einhaltung der Compliance in Exchange durch Litigation Hold oder Retention Policies in der Praxis nicht wirklich umsetzbar. Der Aufwand ist riesig und oft gar nicht durchführbar. Für ein belastbares Löschkonzept bedarf es klarer Berechtigungskonzepte und einer Verfahrensdokumentation.

Im Fall der Compliance Archivierung mit Netmail kann auf Litigation Hold und Retention Policies im Exchange System verzichtet werden. Die lückenlose und revisionssichere Archivierung wird durch das (Cloud-)Archivsystem sichergestellt. Löschungen sind somit unter Rücksichtnahme auf Berechtigungskonzepte und Workflows durchführbar, im Exchange System und im Archivsystem. Es kann zudem sichergestellt werden, dass auf personenbezogene und sensible Daten nur im Mehraugenprinzip zugegriffen und somit erst nach Freigabe z. B. durch den Datenschutzbeauftragten und der internen Revision gelöscht werden kann.

Das Löschen von Daten oder das temporäre Verschieben von Daten in Quarantäne, kann komfortabel On-Premise und in Office 365 durchgeführt werden.

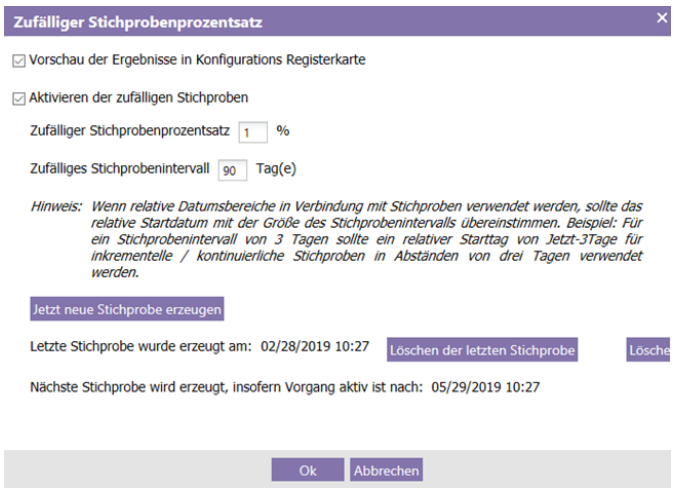
Protokollierte Prüfung eines Verbots privater Nutzung des E-Mail Systems

Viele Unternehmen haben die Auffassung, dass ein ausgesprochenes Verbot der Privatnutzung des E-Mail-Systems ausreicht.

Dies ist jedoch nicht der Fall, denn ohne eine protokollierte, stichprobenartige, regelmäßige Überprüfung der Einhaltung bei zufällig ausgewählten Personen, geht das Verbot in eine Duldung über und damit greifen die Vorschriften des Telekommunikationsgesetzes.

Für die Überprüfung werden wiederum dedizierte Applikationen benötigt, die den spezifischen Anforderungen gerecht werden können.

Netmail unterstützt eine vollständig verwertbare und automatisierte Durchführung solcher Überprüfungen, z. B. in Bezug auf die private E-Mail-Kommunikation. Hierbei kommen KI (Künstliche Intelligenz) und frei konfigurierbare Richtlinien zum Tragen. Mit der zusätzlichen Protokollfunktion sind Unternehmen jederzeit in der Lage Bericht zu erstatten über die durchgeführten Überprüfungen und werden somit einer Nachweispflicht gerecht.



Inaktive Accounts & ausgeschiedene Mitarbeiter

Insbesondere vor dem Hintergrund der Aufbewahrung nach GoBD bzw. möglichen Rechtsstreitigkeiten spielen auch inaktive Accounts bzw. Accounts ausgeschiedener Mitarbeiter eine tragende Rolle. Derzeit sind solche Accounts bei der Nutzung von Office 365 nicht lizenzpflichtig, was einige Unternehmen dazu verleitet, dieses scheinbar großzügige Angebot von Microsoft anzunehmen und zusätzliche Lösungen von Dritt-anbietern aufzugeben. Ein Risiko, dass von vielen Unternehmen unterschätzt wird, denn die Lizenzierung solcher Accounts wird bereits seit geraumer Zeit viel diskutiert. Spätestens wenn Microsoft diese Lizensierung umsetzt, sind Unternehmen gezwungen zu handeln und mitunter horrende Summen zu zahlen. Glücklich schätzen werden sich Unternehmen, die hier bereits vorgesorgt und entsprechende Lösungen im Einsatz haben, wie z.B. das (Cloud-)Archivsystem von Netmail.

Umgang mit personenbezogenen und privaten Daten

Wie bereits vorab beschrieben, sind hinsichtlich des Umgangs mit personenbezogenen und privaten bzw. anderen sensiblen Daten ein entsprechendes Schutzniveau sowie gesonderte Zugriffsrechte umzusetzen. Netmail legte frühzeitig einen Fokus auf diese Thematik und bietet mehrere Möglichkeiten, um den unterschiedlichen Anforderungen gerecht zu werden.

Unternehmen können beispielsweise die getrennte Speicherung der geschäftlichen Daten von personenbezogenen, sensiblen und privaten Daten entsprechend den gesetzlichen Anforderungen umsetzen. Die Daten können dabei logisch oder physikalisch voneinander getrennt abgelegt werden. Auch für die Klassifizierung dieser getrennten Speicherung stehen dem Anwender mehrere Möglichkeiten zur Verfügung.

Die Klassifizierung durch Ablage in unternehmensweit verteilten Ordnern eignet sich insbesondere für empfangene Daten. Auch eine Kategorisierung von E-Mails ist in Exchange (Online) für die getrennte Handhabung der unterschiedlichen Daten möglich und eignet sich für den Anwender insbesondere für gesendete Dateien. Für die Klassifizierung auf unterschiedlichsten Wegen wird dem Anwender ein vom Unternehmen festgelegter Zeitraum vorgegeben (bspw. 3 Wochen, um auch nach einem Urlaub von 2 Wochen oder Krankheit noch die Möglichkeit der Klassifizierung zu gewährleisten). Nach dem festgelegten Zeitraum erfolgt die Regelarchivierung. Die Daten werden dann entsprechend ihrer Klassifizierung archiviert. Dabei können beispielsweise nachfolgende Archivierungslokationen entstehen, die von Unternehmen frei wählbar sind.

Archivierungslokationen, die sensible Daten enthalten, können dabei hinsichtlich des Zugriffs mit einem besonderen Schutzniveau versehen werden. Zugriff ist dabei nur im 4-Augen-Prinzip möglich, für das sich zwei vorab benannte Personen durch separate Passworteingabe authentifizieren müssen. Jeglicher Zugriff wird dabei protokolliert.

Die Rollen für einen solchen Zugriff (sogenannte Case- bzw. Auditmanager) sind bewusst personenbezogen zu definieren, da hierbei mitunter ein hohes Maß an Vertrauen und Verantwortung vorausgesetzt wird. Klassischerweise übernimmt der Datenschutzbeauftragte diese Rolle in Zusammenarbeit mit einem Betriebsratsmitglied bzw. einem Mitarbeiter der internen Revision oder HR.

DLP (Data Leak Prevention)

Da die Thematik des Datenverlustes bzw. des Abhandenkommens sowie das fälschliche Verbreiten von Daten gerade vor dem Hintergrund der DSGVO höchst risikobehaftet ist, sollten Unternehmen Maßnahmen ergreifen, die genau das verhindern. Zeitgleich liegt hierin die Herausforderung, dass viele Unternehmen nicht alle unstrukturierten Daten ausschließlich in Office 365 haben. Mit dem Basis Compliance Modul werden die meisten Unternehmen daher nicht auskommen. Um sich gesetzeskonform und vor allem sicher aufzustellen, lohnt es sich Funktionalitäten und Preise von Drittanbietern mit dem Advanced Compliance Modul zu vergleichen, das sich nach wie vor lediglich auf Dienste in Office 365 beschränkt.

Netmail bietet mit dem Zusatzmodul „Audit & Remediation“ die perfekte Schnittstelle, um diesen Herausforderungen gerecht zu werden. Dabei beschränkt sich Netmail nicht auf Office 365, sondern erlaubt die Integration weiterer Anwendungen sowie des File Systems. E-Discovery Vorgänge im Rahmen von Audits, Datenschutzauskünften und anderen Fällen können so auf einfache Weise umgesetzt werden. Eine KI hinter der Lösung sorgt außerdem automatisiert für die notwendigen Eingriffe, sollten Daten falsch abgelegt oder gar sensible Informationen beispielsweise per E-Mail versendet werden. Automatisch generierte Hinweismails informieren die entsprechenden Personen, wie z. B. den Datenschutzbeauftragten über derartige Vorgänge und geben die Möglichkeit Handlungen freizugeben. Datenverlust bzw. dem Abhandenkommen oder fälschlicher Verbreitung von Daten wird unter Nutzung des Zusatzmoduls vorgebeugt. Das Zusatzmodul von Netmail ist dem Advanced Compliance Modul nicht nur funktionell überlegen, sondern besticht dabei auch mit einem deutlich geringerem Preis.

Compliance Anforderungen und Office 365

Exchange Online, Office 365 und die gesetzlichen Anforderungen an Aufbewahrung (GoBD), Auskunftsfähigkeit und das Recht auf Vergessen (DSGVO)

Netmail EMEA GmbH

Itzbachweg 16-20, 65510 Idstein
+49 6126 5019 525
emea@netmail.com
www.netmail.com