Welche Anforderungen sich hinsichtlich der E-Mail Archivierung ergeben und wie das technisch gelöst werden kann (am Beispiel REDDOXX)

Autor: Jürgen Dagutat, Aurenz GmbH - Geschäftsführer & geprüfter Datenschutzbeauftragter

Auswirkungen der EU-DSGVO auf die E-Mail Archivierung

Am 25. Mai 2018 ist es soweit, die EU Datenschutzgrundverordnung tritt in Kraft. Eine weitestgehende Vereinheitlichung des europäischen Datenschutzrechtes soll damit erreicht werden und wird direkt geltendes Recht in allen Mitgliedsstaaten sein.

Davon betroffen sind alle Organisationen, als auch alle Prozesse eines Unternehmens.

Im Zuge der Datenschutzgrundverordnung wurden auch die Sanktionsmöglichkeiten deutlich verschärft. Bis zu 4% des globalen Jahresumsatzes (oder 20 Mio. EUR) kann ein Bußgeld betragen. Zusammen mit der persönlichen Haftung von Geschäftsführern und Vorständen sollte damit ein noch stärkerer Fokus auf dem Datenschutz liegen.

Ein Bestandteil bei der Umsetzung der DSGVO sollte dabei die E-Mail Archivierung sein.

Welche Aspekte sind bei der E-Mail Archivierung besonders zu beachten?

Wesentliche Bestandteile der Datenschutzgrundverordnung sind ein transparenter Umgang mit personenbezogenen Daten hinsichtlich

- der Erhebung,
- der Speicherung,
- der Verarbeitung,
- dem Zugriff und
- der Löschung.

Auch E-Mails können personenbezogene Daten darstellen oder enthalten. Ohne eine Lösung zur E-Mail Archivierung verfügen viele Unternehmen allerdings kaum über Kontrolle über Ihre E-Mails. Ob E-Mails überhaupt vorhanden sind und wo diese abgelegt sind, ist häufig völlig unklar.

Der Einsatz einer E-Mail Archivierung hilft also dabei, eine einheitliche Ablage für die elektronische Kommunikation im Unternehmen zu erzielen.

Allgemeines

Die folgenden Kurzpapiere der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK) dienen als guter Anlaufpunkt zur ersten Orientierung zum Thema Datenschutz-Grundverordnung (DSGVO):

Kurzpapier Nr. 6: Auskunftsrecht der betroffenen Person, Art.15 DS-GVO
https://www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf

Kurzpapier Nr. 11: Recht auf Löschung / „Recht auf Vergessenwerden“
https://www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf

Kurzpapier Nr. 3: Verarbeitung personenbezogener Daten für Werbung
https://www.lda.bayern.de/media/dsk_kpnr_3_werbung.pdf

Art. 5 DSGVO – Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen...

...auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

...in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Der Verantwortliche ist für die Einhaltung verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 5 DSGVO am Beispiel REDDOXX

Die archivierten E-Mails werden von der REDDOXX Appliance in verschlüsselten Archiv-Containern auf einem vom Kunden definierten Speicherort abgelegt. Diese Container sind mit dem Algorithmus „AES256“ verschlüsselt, so dass die E-Mails auf dem Speicherort nicht im Klartext einsehbar sind.

Das Berechtigungskonzept der REDDOXX Appliance sieht vor, dass jeder Mitarbeiter im Archiv nur Zugriff auf seine eigenen E-Mails hat. Die Autorisierung des Anwenders erfolgt dabei gegen einen Verzeichnisdienst, im Regelfall gegen die im Active-Directory vorhandenen Benutzerkonten. Die sogenannte Basisberechtigung ergibt sich durch Verwendung der im Verzeichnisdienst vorhandenen Aliastabellen. Daraus resultiert, dass der Mitarbeiter ***Dieter Datenschutz*** nur Zugriff auf archivierte E-Mails erhält, deren Absender oder Empfänger seiner E-Mailadresse ***dieter.datenschutz@firma.de*** entspricht, was einer angemessenen Sicherheit vor unbefugtem Zugriff entspricht.

Werden E-Mails aus dem Archiv heraus in das EML-Format exportiert (Datenübertragbarkeit, siehe nächste Seite), gibt es keine weiteren Schutzmechanismen, um ein Lesen der E-Mails zu verhindern. Dies resultiert daraus, dass es sich bei dem EML-Format um ein Standardformat von E-Mails handelt, was für eine eventuelle Weiterverwendung notwendig ist.

Alternativ zum Export besteht die Möglichkeit, E-Mails in einen separaten Archiv-Container zu kopieren und diesen Offline zur Verfügung zu stellen. Das Öffnen von diesem verschlüsselten Archiv-Container kann mit einem zusätzlichen Passwort abgesichert werden.

Art. 15 DSGVO – Auskunftsrecht der betroffenen Person

Jedes Unternehmen muss ab 2018 gespeicherte Daten ihrer Kunden, Lieferanten, Hersteller etc. auf Wunsch herausgeben und zwar in einem Datenformat, das von einem anderem Dienstleister leicht weiterverwendet werden kann (Datenübertragbarkeit).
Betroffene Personen haben das Recht von einem Verantwortlichen Auskunft über sie betreffende, personenbezogenen Daten zu verlangen und ob diese Daten verarbeitet wurden oder werden.

Auch eine Negativauskunft ist zu erbringen, falls der Verantwortliche keine Daten zur betreffenden Person hat oder diese unumkehrbar anonymisiert wurden.

Darüber hinaus kann die betroffene Person Auskunft verlangen, welche personenbezogenen Daten verarbeitet wurden oder werden. Diese Informationen beinhalten unter anderem:

- Verarbeitungszwecke
- Empfänger der Daten
- voraussichtliche Speicherungsdauer
- Herkunft der Daten
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung
- Rechte des Widerrufs

Art. 15 DSGVO am Beispiel REDDOXX

Herkunft und ***Empfänger*** stellen bei einer E-Mail den Absender und Empfänger dar und sind dementsprechend einfach zu beauskunften. Darüber hinaus können im Regelfall dem Inhalt der archivierten E-Mail weitere Informationen entnommen werden.

Der ***Verarbeitungszweck*** lässt sich häufig dem Inhalt der E-Mail entnehmen, da sich dieser auf etwas bezieht (Angebot, Anfrage, Teilnahme am Gewinnspiel, Bewerbung, etc.). Weiterführend lassen sich sowohl der ***Verarbeitungszweck****,* als auch die ***voraussichtliche Speicherdauer*** dem Compliance-Framework der REDDOXX Appliance entnehmen, in dem unterschiedliche Aufbewahrungszeiten definiert werden können. Dies kann pauschal (z.B. E-Mails aus dem Jahr 2017 für mindestens 11 Jahre nicht löschbar) oder inhaltsbezogen (z.B. E-Mails mit einem PDF-Anhang als Rechnung behandeln und 11 Jahre nicht löschbar, wenn in dem PDF die Begriffe „Rechnungsnummer“, „Ihre Bestellung vom“, etc. vorkommen) erfolgen.

Das ***Löschen*** von E-Mails ist je nach Berechtigung durch einzelne User und/oder den Administrator möglich. Die Löschung kann durch ein Mehr-Augen-Prinzip abgesichert werden und wird in jedem Fall protokolliert.

Die ***Datenübertragbarkeit*** lässt sich durch einen Export von den relevanten E-Mails in das EML-Format ermöglichen. Dabei handelt es sich um das native Ursprungsformat von E-Mails, so dass sich diese mit jedem gängigen Mailclient (Outlook, Thunderbird, etc.) öffnen lassen und so die Datenübertragbarkeit gewährleistet wird.

Autor: Jürgen Dagutat, Aurenz GmbH - Geschäftsführer und geprüfter Datenschutzbeauftragter
Bildquelle Titelbild: Alexander Limbach / Fotolia.com

Art. 17 DSGVO – Recht auf Löschung („Recht auf Vergessenwerden“)

Die betroffene Person hat das Recht, die unverzügliche Löschung von personenbezogenen Daten zu verlangen.

Der Verantwortliche ist verpflichtet, dieser Aufforderung nachzukommen, sofern einer der folgenden Gründe zutrifft:

- die Notwendigkeit der Verarbeitung zur Erfüllung eines Zweckes ist nicht mehr gegeben
- die betroffene Person hat ihre Einwilligung widerrufen
- die betroffene Person legt Widerspruch gegen die Verarbeitung ein
- die personenbezogenen Daten wurden unrechtmäßig verarbeitet

Art. 17 DSGVO am Beispiel REDDOXX

Das Löschen von E-Mails ist je nach Berechtigung durch einzelne User und/oder den Administrator möglich. Die Löschung kann durch ein Mehr-Augen-Prinzip abgesichert werden und wird in jedem Fall protokolliert.

Ein Beispiel für manuelles Eingreifen durch einen User stellen Bewerbungen dar. Sollen nach Abschluss eines Bewerbungsverfahrens die Unterlagen der abgelehnten Bewerber entfernt werden, kann dies ein Automatismus im Regelfall nicht leisten, da dieser nicht weiß, wer eingestellt wurde und wer nicht.
Um Bewerbungen zu entfernen, könnte einem Mitarbeiter aus dem Personalwesen die Berechtigung eingeräumt werden, E-Mails innerhalb des Archivbestandes als abgelehnte Bewerbung zu markieren. Soll ein Missbrauch dieser Funktion verhindert werden, kann ein Mehr-Augen-Prinzip etabliert werden. Hier müssen 1-n Personen der Löschung zustimmen, bevor sie vollzogen wird.
Sowohl die Markierung als auch die Zustimmung werden im Compliance LOG der REDDOXX Appliance protokolliert.

Neben dem manuellen Zuordnen von E-Mails besteht auch die Möglichkeit, die betreffenden E-Mails über einen Automatismus zu löschen. Welche E-Mails durch die Löschroutine aus dem Archiv entfernt werden, kann dabei frei definiert werden.
So könnten beispielsweise alle E-Mails einer Person entfernt werden, wenn der Sender oder Empfänger ***dieter.datenschutz@firma.de*** lautet. Zusätzlich ist es möglich, das Archiv über die Volltextsuche nach dem Namen der betroffenden Person zu durchsuchen, um die dabei gefundenen E-Mails zu entfernen.

Wichtig: Die E-Mails werden nicht gelöscht, sofern sie einer Mindestaufbewahrungszeit unterliegen (weil sie z.B. eine Rechnung darstellt und aus steuerrechtlichen Gründen für 11 Jahre vorgehalten werden soll).