E-Mail-Archivierung und Datenschutz

Was Sie jetzt wissen müssen

Welcher Zusammenhang besteht zwischen den Themen „E-Mail-Archivierung“ und „Datenschutz“?

Die “Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff” (kurz GoBD) schreiben die manipulationssichere Archivierung aller geschäftskritischen E-Mails vor. In Sachen Datenschutz bedeutet das zum einen, dass eine E-Mail-Archivierung zu einem sauberen, nachvollziehbaren Datenmanagement beiträgt – wie es beispielsweise auch in der Datenschutz-Grundverordnung gefordert wird. Zum anderen heißt es aber auch, dass beispielsweise E-Mails privaten Inhalts oder Bewerbungen gesondert zu behandeln sind, um dem Datenschutz hier gerecht werden zu können.

Welchen Beitrag leistet die E-Mail-Archivierung zur Einhaltung der DSGVO?

Die Datenschutz-Grundverordnung definiert übergreifend die Grundlagen für eine rechtskonforme Datenverarbeitung – und erlegt damit auch der E-Mail-Archivierung Rahmenbedingungen auf. Als Beispiele seien hier angemessene Schutzmaßnahmen zur Datensicherheit – wie Zugriffs-Management oder Verschlüsselung – oder das Recht auf Vergessenwerden – also das Löschen entsprechender Datensätze – genannt.

Gleichzeitig ermöglicht eine durchdachte E-Mail-Archivierung es, geschäftliche Absprachen, Angebote und Abschlüsse transparent und nachvollziehbar aufzubewahren – zum einen erfüllen Unternehmen so eine rechtliche Pflicht, zum anderen ist ein sauberes Datenmanagement ein unverzichtbarer Baustein zur DSGVO-Konformität.

Denn ein intuitiv durchsuchbares und strukturiertes Archiv unterstützt Unternehmen in Sachen Auskunftsfähigkeit, während automatisiert gepflegte und verfolgte Aufbewahrungsfristen dazu beitragen, organisatorische Prozesse wie die Handhabung von Bewerbungen datenschutzrechtlich korrekt zu gestalten und das Recht auf Vergessenwerden zu wahren.

Die E-Mail-Archivierung ist gesetzlich vorgeschrieben. Wie schaffen Unternehmen den Spagat zwischen dieser Pflicht und dem Datenschutz?

Um die Nachvollziehbarkeit geschäftlicher Prozesse lückenlos zu gewährleisten, sollten E-Mails automatisch beim Eintreffen archiviert und im Idealfall aus dem Produktivsystem entfernt werden, sobald sie ihren Zweck – wie beispielsweise eine Terminabsprache oder einen Vertragsabschluss – erfüllt haben.

Die DSGVO gibt hierbei jedoch übergeordnete Rahmenbedingungen vor, die teilweise ein Spannungsverhältnis zur Archivierungspflicht entstehen lassen. So gilt es beispielsweise, die unterschiedlichen Aufbewahrungsfristen bei verschiedenen Inhalten zu bedenken und einzuhalten. Enden diese, müssen Unternehmen sie entsprechend der Rechenschaftspflicht mittels eines prüf- und nachvollziehbaren Löschprozesses aus dem Archiv entfernen.

Auch Artikel 25 der DSGVO zum "Datenschutz durch Technikgestaltung" stellt Anforderungen an das E-Mail-Archiv. So sollten archivierte Nachrichten sowie beigefügte Dokumente durch Zugriffskontrollen – beispielsweise via Passwort oder singuläre Administratorenrechte – oder Verschlüsselung vor fremder, unbefugter Einsichtnahme geschützt werden.

Letztlich bewegt sich das E-Mail-Archiv auch im Verhältnis zum Backup und sollte entsprechend des Artikels 32, der die "Sicherheit der Verarbeitung" fordert, entsprechend in der Backup-Strategie berücksichtigt werden. Denn die DSGVO fordert von Unternehmen umfassende Maßnahmen, um die Verfügbarkeit der Daten auch bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen – das schließt auch E-Mails mit ein.

Wie behandeln Unternehmen private Mails, die über den Firmen-Account versendet werden?

Private Nachrichten und E-Mail-Archivierung stehen sich in einem spannungsgeladenen Verhältnis gegenüber: Wenn private Nachrichten über die automatische Archivierung in das E-Mail-Archiv gelangen, unterliegt dieses automatisch dem Paragraf 88 des Telekommunikationsgesetzes – dem Post- und Fernmeldegeheimnis. Damit darf das Archiv nicht mehr eingesehen werden, ohne dass eine Einverständniserklärung des Betroffenen vorliegt. Auch eine Betriebsvereinbarung reicht hier nicht aus, um sich über das Fernmeldegesetz hinwegzusetzen.

Am verlässlichsten werden solche Fälle von vornherein ausgeschlossen, wenn Unternehmen private Kommunikation über die Firmenadresse vollständig untersagen. Alternativ ist auch eine freiwillige Einwilligung zur Einsichtnahme möglich, die vorab beim Einstellungsgespräch unterzeichnet wird – die aber nicht als Bedingung zur Einstellung gelten darf, da sonst nicht von Freiwilligkeit gesprochen werden kann.

Wie gehen Unternehmen mit Bewerbungen via E-Mail um? Was ist hier zu beachten?

Bewerbungen stehen ebenfalls in einem Spannungsverhältnis zwischen gesetzeskonformer E-Mail-Archivierung und Datenschutz: Während sie als solche nicht zur geschäftlichen Kommunikation zählen und damit nicht der GoBD unterliegen, werden sie doch bei einem rechtskonform aufgesetzten Archivierungs-mechanismus automatisch bei Eingang archiviert.

Bei der Frage nach dem weiteren Vorgehen in diesen Fällen wird der Ansatz der Verhältnismäßigkeit herangezogen: In der Regel wird der Aufwand, um Bewerbungen von der automatischen Archivierung auszuschließen, als zu groß erachtet, um praktikabel zu sein – besonders gemessen an dem Risiko, dem der betroffene Bewerber im Falle einer Datenschutzverletzung ausgesetzt ist. Dieses Risiko wird auch deshalb als niedrig eingestuft, da das Archiv lediglich mit Begründung auf die GoBD eingesehen werden darf.

Hinzu kommt, dass eine Archivierung von Bewerbungen für Unternehmen durchaus sinnvoll ist, denn über einen Zeitraum von bis zu sechs Monaten können Bewerbungsunterlagen als Beweismittel herangezogen werden, sollte ein Bewerber gerichtlich gegen eine Ablehnung vorgehen. Hierzu kann ein zweites Archiv aus Gründen der Arbeitsorganisation aufgebaut werden, dass nicht automatisch am Gateway sondern nach Bedarf archiviert und aus dem Nachrichten entfernt werden können – Bewerbungen beispielsweise sollten nach Ablauf dieser Frist gelöscht werden.

Was ist bei E-Mail-Archivierung as a Service zu bedenken?

Managed Service Provider gelten vor der DSGVO als datenverarbeitende Auftragnehmer, deren Kunden entsprechend als datenverantwortlicher Auftraggeber. Damit muss zwischen diesen beiden Parteien eine “Vereinbarung zur Verarbeitung im Auftrag” (VVA) geschlossen werden, welche den Datenumgang regelt und den -schutz gewährleisten soll. Als Datenverantwortlicher legt der Kunde die Inhalte fest, während der MSP verpflichtet ist, diese auf die Notwendigkeit einer VVA hinzuweisen.

Fazit zum Thema „E-Mail-Archivierung & Datenschutz“

Die Themen E-Mail-Archivierung und Datenschutz sind ineinander verzahnt zu betrachten: Die Archivierung geschäftskritischer E-Mails ist rechtlich in der GoBD gefordert und trägt dabei zu einem transparenten und nachvollziehbaren Daten-Management bei. Gleichzeitig stellt jedoch die DSGVO Regeln zur Ausgestaltung und Verwaltung des Archivs auf, die es erforderlich machen, Nachrichtenverläufe in Unternehmen zu strukturieren und – im Falle privater Nachrichten – zu reglementieren. Erreicht werden kann dies nur durch einen Maßnahmen-Mix in Sachen E-Mail-Kommunikation, Security und organisatorischen Policies.

Um hier bereits den grundlegenden Baustein sicher zu platzieren, ist eine professionelle E-Mail-Archivierungs-lösung unerlässlich, die auf der einen Seite die rechtlichen Ansprüche erfüllt und auf der anderen Seite ausreichend Möglichkeiten zum datenschutzkonformen Archiv-Management bereithält.