Erdem Durmus, Annika Selzer, Ulrich Pordesch*

Das Löschen nach der DSGVO

Eine Diskussion der datenschutzkonformen Umsetzung bei E-Mails

Die DSGVO schreibt Verantwortlichen vor, personenbezogene Daten nach Erreichung des Zwecks ihrer Verarbeitung zu löschen. Einer Löschpflicht stehen häufig zahlreiche (spezial-) gesetzliche Aufbewahrungspflichten gegenüber. In der betrieblichen Praxis ist die E-Mail eines der wichtigsten Kommunikationsmittel, das gezielte Bewerten und Löschen von tausenden E-Mails stellt jedoch eine komplexe Herausforderung dar. Der Beitrag diskutiert verschiedene Lösungsmöglichkeiten, diese Herausforderung zu meistern.

1 Problemstellung

Die DSGVO schreibt Verantwortlichen vor, personenbezogene Daten nach Erreichung des Zwecks ihrer Verarbeitung zu löschen. Diese Pflicht zur Löschung findet sich an mehreren Stellen des Gesetzes wieder und stellt eine grundsätzliche Anforderung an die rechtmäßige Verarbeitung von personenbezogenen Daten dar.

In der betrieblichen Praxis ist die E-Mail eines der wichtigsten Kommunikationsmittel. In vielen Unternehmen und Forschungseinrichtungen werden über E-Mails Aufträge erteilt und bearbeitet, Unteraufträge vergeben, Ergebnisse mitgeteilt, Patentvorhaben vorbereitet u.v.m. Mitarbeitende erhalten je nach Aufgabenzweck zwischen 20 und 200 E-Mails am Tag, oft zu verschiedenen Zwecken und Themen.

Sowohl die Kopfzeile einer E-Mail wie auch der Nachrichtentext und ggf. Anhänge enthalten i.d.R. personenbezogene Daten, mitunter sogar besondere Kategorien personenbezogener Daten, so dass die datenschutzrechtlichen Löschpflichten im Kontext von E-Mail-Anwendungen anwendbar sind. Allerdings stellt die schiere Masse an E-Mails Verantwortliche in Bezug auf die Umsetzung von Lösch- und Aufbewahrungspflichten vor große Herausforderungen. Im Folgenden sollen daher verschiedene Möglichkeiten diskutiert werden, den Herausforderungen des datenschutzkonformen Löschens von E-Mails zu begegnen.[2]

Erdem Durmus (LL.M.), CIPP/E

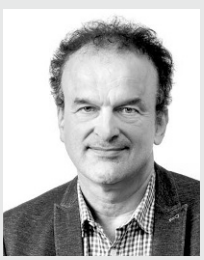
ist externer Datenschutzbeauftragter bei der NOTOS Xperts GmbH in Darmstadt.

E-Mail: durmus@notos-xperts.de

Annika Selzer

ist Wissenschaftlerin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

E-Mail: annika.selzer@sit.fraunhofer.de



Dr. Ulrich Pordesch

ist Informationssicherheits- und Datenschutzkoordinator der Fraunhofer Gesellschaft.

E-Mail: ulrich.pordesch@zv.fraunhofer.de

2 Rechtliche Vorgaben

2.1 Löschpflichten

Die Grundsätze der Verarbeitung nach Art. 5 Abs. 1 DSGVO normieren u.a. die Speicherbegrenzung. Nach Art. 5 Abs. 1 lit. e DSGVO muss der Verantwortliche personenbezogene Daten

* Dieser Artikel gibt die persönliche Sicht der Autoren wieder und ist keine Stellungnahme der Fraunhofer Gesellschaft oder der NOTOS Xperts GmbH.

1 Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit unterstützt. Er entstand in Zusammenarbeit mit der Informationssicherheits- und Datenschutz-Koordination der Fraunhofer Gesellschaft.

2 Der Aufsatz betrachtet keine Fragestellungen, die sich auf das Verbot oder die Erlaubnis der privaten Mitbenutzung der beruflichen E-Mail-Adresse beziehen.

in einer Form speichern, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Ausnahmen hiervon gibt es lediglich für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke (Art. 5 Abs. 1 lit. e 2 HS, Art. 89 DSGVO).

Eine weitere Pflicht des Verantwortlichen zur Löschung von personenbezogenen Daten kann sich aus Art. 17 DSGVO ergeben. Die betroffene Person kann vom Verantwortlichen verlangen, dass Daten zu ihrer Person unverzüglich gelöscht werden, sofern bestimmte, in Art. 17 Abs. 1 DSGVO genannte Gründe zutreffen. Diese Gründe sind u.a. die mangelnde Erforderlichkeit der personenbezogenen Daten für die Zwecke ihrer Verarbeitung, der Widerruf einer erteilten Einwilligung, der Widerspruch gegen eine Verarbeitung oder bspw. eine gesetzliche Löschpflicht.

2.2 Aufbewahrungspflichten

Einer Löschpflicht stehen häufig zahlreiche (spezial-)gesetzliche Aufbewahrungspflichten gegenüber. Bestehen für Daten (spezial-)gesetzliche Aufbewahrungspflichten, die sich über einen längeren Zeitraum erstrecken als der datenschutzrechtliche Zweck, so sind Daten bis zum Ablauf der längsten für sie einschlägigen Aufbewahrungspflicht vorzuhalten.

U.a. spielen das Handels- und Steuerrecht eine wesentliche Rolle bei der Ermittlung rechtlicher Aufbewahrungspflichten. Die §§ 238, 257 HGB verpflichten Unternehmen zur Aufbewahrung von handelsrechtlich relevanten Unterlagen, zu denen u.a. Handelsbücher, empfangene Handelsbriefe sowie Buchungsbelege zählen. § 147 Abs. 1 AO regelt Aufbewahrungsfristen für bestimmte steuerrechtlich relevante Unterlagen. In beiden Fällen, in denen Handelsbriefe bzw. Unterlagen heute sehr häufig E-Mails sind, ergeben sich 6-10jährige Aufbewahrungsfristen [1]. Darüber hinaus können Verjährungsfristen zumindest indirekt eine Aufbewahrung erfordern. Die regelmäßige Verjährungsfrist beträgt gem. § 195 BGB drei Jahre und gilt grundsätzlich für alle Ansprüche des BGB, sofern sie nicht unverjährbar sind oder besonderen Verjährungsfristen unterliegen. Beispiele für solche Ansprüche sind die Rückgewähr des Kaufpreises sowie Ansprüche aus dem Arbeitsvertrag, wie bspw. der Anspruch auf Aushändigung eines Arbeitszeugnisses [9].

2.3 Umsetzung in E-Mail-Anwendungen

E-Mails stellen keine eigene Datenkategorie dar, für die es spezielle rechtliche Anforderungen hinsichtlich der Löschung oder Aufbewahrung gibt. Daher unterliegen sie den allgemeinen gesetzlichen Vorgaben.[3] Es müsste also am Inhalt einer E-Mail festgemacht werden, wie lange sie aufbewahrt bzw. wann sie gelöscht werden kann. Ein grundsätzliches Problem bei der Aufbewahrung von E-Mails ist daher die Feststellung der aufbewahrungswürdigen Inhalte. In der unternehmerischen Praxis stellt dies häufig ein Problem dar, weil es Mitarbeitern schwerfällt, zu definieren oder jemanden anderes definieren zu lassen, was eine aufbewahrungswürdige E-Mail ist, und was nicht. Diese Verunsicherung führt zu einer Neigung der Mitarbeiter, jede E-Mail für lange Zeit aufzubewahren [11]. Gesucht sind daher pragmatische und dem Risiko angemessene Lösungen für die Löschung von E-Mails. Bei der Diskussion möglicher Lösungswege gehen die Autoren davon aus, dass die meisten Unternehmen und Forschungseinrichtungen i.d.R. projektbezogen arbeiten.

3 Kriterien für das Löschen von E-Mails

Bevor Möglichkeiten zur Umsetzung der Löschvorgaben bei E-Mails vorgestellt und diskutiert werden können, ist zunächst zu überprüfen, an welchen Kriterien sich diese messen lassen müssen.

3.1 Angemessenheit als Orientierungspunkt für eine datenschutzkonforme Löschlösung

Art. 24 Abs. 1 DSGVO[4] regelt, dass der Verantwortliche geeignete und angemessene technische und organisatorische Maßnahmen einsetzen muss, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. In dieser Formulierung ist die zentrale Pflicht des Verantwortlichen enthalten, ein wirksames Kontrollsystem zu etablieren, das auch als Datenschutz-Management bezeichnet werden kann.

Der Begriff der technischen und organisatorischen Maßnahmen gem. Art. 24 DSGVO ist weit zu verstehen. Verbindliche Mindeststandards gibt es nicht, maßgeblich ist, dass die getroffenen Maßnahmen objektiv überprüfbar, nachvollziehbar und auf Anforderung nachweisbar sind [2]. Es müssen aber nur verhältnismäßige Vorkehrungen getroffen werden, die in Bezug auf die konkreten Umstände der Verarbeitung und den Verantwortlichen *angemessen* sind. Diesen risikobasierten Ansatz der DSGVO verdeutlichen sowohl Art. 24 Abs. 1 als auch Art. 24 Abs. 2 DSGVO. Die eingesetzten Maßnahmen müssen demnach gem. Art. 24 Abs. 1 DSGVO dem Umfang und dem Zweck der Verarbeitung entsprechen, gleichzeitig muss eine Risikobewertung für die Rechte und Freiheiten der betroffenen Personen durchgeführt werden. Auch die in Art. 24 Abs. 2 DSGVO normierten „geeigneten Datenschutzvorkehrungen" sind zu treffen, sofern dies in einem *angemessenen* Verhältnis zu den Verarbeitungstätigkeiten steht.

Der risikobasierte Ansatz der DSGVO darf aber nicht so missverstanden werden, dass Maßnahmen nur bei Vorliegen von (hohen) Risiken zu treffen wären und der Verantwortliche bei Nichtvorliegen von Risiken von der Pflicht befreit wäre. Vielmehr sind die Maßnahmen unter Beachtung des Verhältnismäßigkeitsgrundsatzes den Risiken entsprechend einzusetzen. Der risikobasierte Ansatz verfolgt das Ziel, eine Ausdifferenzierung der Datenschutzpflichten zu erreichen. Mit strukturierten Risikobewertungen könnte die Komplexität der Anforderungen praktikabler gemacht werden, um ein vernünftiges Aufwand-Nutzen-Verhältnis herstellen zu können [4, 7].

3 E-Mail-Dienste sind Telekommunikationsdienste i.S.d. TKG, in Bezug auf die E-Mail-Nutzung in/durch Unternehmen ergeben sich aus dem TKG jedoch keine besonderen Löschpflichten.

4 Die in Art. 24 DSGVO normierten allgemeinen Vorgaben stellen eine Generalklausel dar. Auch wenn für die Beurteilung der Geeignetheit und Angemessenheit von Maßnahmen in Bezug auf die Löschung hauptsächlich die Generalklausel des Art. 24 DSGVO Anwendung findet, können sich ggf. auch aus Art. 25 DSGVO Anforderungen an die zukünftige Ausgestaltung technischer Systeme in Bezug auf die Löschung von E-Mails ergeben.

3.2 Ermittlung der Risiken der Verarbeitung

In die Bewertung der Angemessenheit der Maßnahmen zur Löschung von E-Mails muss also sowohl die Bewertung in Bezug auf die Risiken der Verarbeitung für die Rechte und Freiheiten der betroffenen Person sowie zum anderen eine Verhältnismäßigkeitsprüfung zugunsten des Verantwortlichen einfließen. Verantwortliche müssten sich also überlegen, welche personenbezogenen Daten in den E-Mails regelmäßig verarbeitet werden und eine Schutzbedarfsfeststellung für diese Daten durchführen [5].

Der potenzielle Eintritt eines Risikos für die betroffene Person ist aber auch von verarbeitungsbezogenen Kriterien abhängig, wie etwa von der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung, so wie dies auch in Art. 24 Abs. 1 genannt wird. Aus dem Umfang allein lässt sich ein hohes Risiko der Verarbeitung noch nicht ableiten, die Schwere eines Eingriffs in Persönlichkeitsrechte der betroffenen Person misst sich vielmehr daran, welche Informationen sich aus den Daten gewinnen lassen und worin ihre konkrete Verwendung liegt [4]. Es kann also gesagt werden, dass die hohe Anzahl an ein- und ausgehenden E-Mails nicht automatisch eine Verarbeitung mit höherem Risiko begründen.

Die Zwecke der Verarbeitung haben ebenfalls Einfluss auf die Schwere des Eingriffs und somit auf die Höhe des Risikos für die betroffene Person. So kann eine Verarbeitung stets als risikoreicher betrachtet werden, wenn sie zu Zwecken des Profilings erfolgt, um persönliche Aspekte der betroffenen Person zu bewerten, oder wenn personenbezogene Daten zu Zwecken von Analysen oder Auswertungen verarbeitet werden sollen [4, 5]. Die genannten Aspekte greifen jedoch i.d.R. im Anwendungskontext der geschäftlichen E-Mail-Kommunikation nicht: die geschäftliche E-Mail-Kommunikation findet i.d.R. nicht statt, um primär personenbezogene Daten zu verarbeiten, anders als bspw. bei einer Kundendatenbank zur Pflege der Kundenbeziehungen, in welcher die Kontaktdaten von Tausenden Kunden enthalten sind. Potentiell gefährlichere Verarbeitungstätigkeiten, wie etwa das Profiling oder Verarbeitungen zu Zwecken der Datenanalyse, können ausgeschlossen werden. Die Kommunikation unter Verwendung der E-Mail findet schlichtweg nicht zu diesen Zwecken statt.

Auch die verarbeiteten Datenkategorien bergen im Anwendungsbereich der geschäftlichen E-Mail-Kommunikation i.d.R. kein hohes Risiko: in E-Mails sind im Regelfall nur besondere Kategorien von personenbezogenen Daten in geringerem Umfang enthalten, bspw., wenn E-Mail-Adressen in Unternehmen für die Zusendung von Bewerbungen und Bewerbungsunterlagen eingerichtet wurden und Bewerbungen z.B. Informationen zum Schwerbehindertenstatus eines Bewerbers enthalten. Die Anzahl der E-Mails, die besondere Kategorien von personenbezogenen Daten i.S.d. Art. 9 Abs. 1 DSGVO enthalten, ist im Verhältnis zur Gesamtzahl aller E-Mails aber i.d.R. gering.

Eine weitere Herangehensweise an die Ermittlung des Risikos, die unter die Umstände der Verarbeitung subsumiert werden kann, ist die Bestimmung der wirtschaftlichen Verwertbarkeit der personenbezogenen Daten sowie vertraglicher oder gesetzlicher Verpflichtungen [10]. E-Mails im Zusammenhang mit abgeschlossenen Projekten werden im Regelfall zu Nachweiszwecken oder zur Gewährleistung vertraglicher Ansprüche aufbewahrt. Ein primäres wirtschaftliches Interesse an den Daten selbst ist meistens nicht vorhanden. Zwar könnte ein wirtschaftliches Interesse an den Kontaktdaten der Vertragspartner bestehen, aber in Unternehmen werden solche Daten meistens umgehend in CRM-Datenbanken überführt, die für solche Zwecke der Kundenpflege gedacht sind. Insofern würden die gleichen Informationen, die zusätzlich in einer E-Mail vorhanden sind, keinen wirtschaftlichen Mehrwert haben.

Bei in E-Mails enthaltenen personenbezogenen Daten kann im Ergebnis grundsätzlich von einem eher geringen Risiko der Verarbeitung für die Rechte und Freiheiten der betroffenen Personen ausgegangen werden. Ausnahmen bestehen insbesondere dann, wenn E-Mail-Adressen in Unternehmen für bestimmte Zwecke der Kommunikation eingerichtet wurden, in deren Rahmen besondere Kategorien personenbezogener Daten verarbeitet werden sollen, was z.B. bei einer Funktionsadresse für die Zusendung von Bewerbungen der Fall wäre, bei der Bewerber u.a. Angaben zum Schwerbehindertenstatus machen können.

4 Vorschlag zum Löschen von E-Mails

Das Ergebnis der Risikobewertung ist nun auf verschiedene Umsetzungsmaßnahmen zur Löschung von E-Mails anzuwenden, um die Angemessenheit dieser Maßnahmen einschätzen zu können.

4.1 Individuelles Sichten und Löschen

Es ist zunächst fraglich, ob Unternehmen bzw. ihre Mitarbeiter jede einzelne empfangene und versendete E-Mail in ihrem Postfach sichten und einzelfallabhängig auf Grundlage der in der E-Mail enthaltenen personenbezogenen Daten eine Entscheidung hinsichtlich des Löschzeitpunkts treffen müssten.

Die Angemessenheit dieses Vorgehens ist zu verneinen. Zwar ist die organisatorische Maßnahme der individuellen Sichtung jeder einzelnen versendeten und empfangenen E-Mail geeignet, um auf dieser Basis Löschungen vorzunehmen. Diese Maßnahme ist allerdings in Relation zu der schieren Masse an in den Postfächern der Mitarbeiter vorhandenen E-Mails, dem u.U. großen Umfang bereits einer einzelnen E-Mail einschließlich ihrer Anhänge, nicht angemessen.

Für die überwiegende Mehrheit der in den E-Mails enthaltenen personenbezogenen Daten wurde ein geringes Risiko für die Rechte und Freiheiten der betroffenen Personen festgestellt. In E-Mails sind in deutlich geringerem Umfang besondere Kategorien von personenbezogenen Daten enthalten. Auch vor diesem Hintergrund wäre diese Maßnahme also nicht angemessen, zumal sie für ein insgesamt geringfügiges Risiko einen unverhältnismäßig hohen Aufwand erfordern würde.

Neben dem großen organisatorischen und zeitlichen Aufwand besteht für den Verantwortlichen darüber hinaus die Gefahr, dass Mitarbeiter E-Mails fehlerhaft löschen. Dies ist insbesondere bei E-Mails zu Nachweis- und Dokumentationszwecken ein wirtschaftliches Risiko des Verantwortlichen. Wenn etwa eine steuerrechtlich aufbewahrungsbedürftige E-Mail vor Ablauf der Aufbewahrungsfrist gelöscht wird, darf das Finanzamt gem. § 162 Abs. 1 S. 1 AO die Besteuerungsgrundlage für fehlende Unterlagen schätzen. Die Löschung von patentrechtlich relevanten E-Mails kann im schlimmsten Fall zum Verlust eines Patentes führen, wenn dadurch wichtige Nachweise verloren gehen.

Aus diesen Gründen sollten alternative Maßnahmen zur Realisierung der Löschung von E-Mails herangezogen werden.

4.2 „Pauschales" Löschen

Verantwortliche könnten eine Löschung von E-Mails dahingehend praktikabel umsetzen, indem sie die längste, für sie anwendbare Aufbewahrungsfrist ermitteln, die im Rahmen des Versendens und Empfangens von E-Mails für das Unternehmen zu beachten ist und ermitteln, ob zu diesem Zeitpunkt auch der datenschutzrechtliche Zweck der Verarbeitung erfüllt ist und die Umsetzung der Löschpflichten im Rahmen von E-Mail-Anwendungen sodann auf Basis dieser längsten Aufbewahrungsfrist durchführen. Ermittelt der Verantwortliche etwa als längste Aufbewahrungsfrist die 10-jährige Aufbewahrungspflicht aus §§ 257 Abs. 4 HGB, 147 Abs. 3 AO, so könnte eine praktikable und angemessene Umsetzung der Löschpflichten darin bestehen, alle E-Mails nach Ablauf von 10 Jahren zu löschen, sofern auch der datenschutzrechtliche Zweck nach diesem Zeitraum erfüllt ist.

Die Angemessenheit dieses Vorgehens ist zu verneinen, da bei der Umsetzung dieser Maßnahme eine Ausdifferenzierung der Risiken für die betroffene Person nicht stattfinden würde [4, 8]. Alle E-Mails würden gleich behandelt werden, was mit dem risikobasierten Ansatz der DSGVO nicht vereinbar wäre. Der Verantwortliche ist verpflichtet, den Risiken entsprechende Maßnahmen einzusetzen. Im Vordergrund des risikobasierten Ansatzes steht der Schutz der betroffenen Person [5, 7].

Betroffene Personen haben ein Interesse daran, dass insbesondere besonders sensible Informationen nicht „zu lange" aufbewahrt werden. Doch diese Maßnahme sieht eben keine Bewertung der Sensibilität der Informationen vor. Stattdessen werden alle E-Mails „gleichgesetzt" und unter eine gemeinsame Aufbewahrungsfrist zusammengefasst. Auch wenn diese Maßnahme für den Verantwortlichen keinen Nachteil mit sich bringt, kann sie aus der Perspektive der betroffenen Person nicht geeignet und angemessen sein, um die datenschutzrechtlichen Anforderungen an die Löschung umzusetzen.

4.3 Archivieren und feste Löschzeitpunkte

Nachdem weder die Vorgehensweise des individuellen Sichtens jeder einzelnen E-Mail noch das pauschale Löschen von Mails nach Ablauf der längsten Aufbewahrungspflicht zur Umsetzung der Löschung angemessen sind, müsste eine alternative Lösung gefunden werden, die geeignet und angemessen i.S.d. Art. 24 Abs. 1 DSGVO ist. Als Vorgehensweise empfiehlt sich die Umsetzung von Maßnahmen, die einen „Kompromiss" zwischen den beiden eben vorgestellten, als nicht angemessen eingeschätzten Lösungswegen darstellt.

Hierfür wäre denkbar, die ein- und ausgehenden E-Mails je E-Mail-Postfach in drei Arten zu ordnen:

- E-Mails, die zum Schutz der betroffenen Personen nach besonders kurzer Zeit gelöscht werden müssen,[5]
- E-Mails, die aus schutzwürdigen Interessen des Verantwortlichen besonders lange aufbewahrt werden müssen
- alle anderen ein- und ausgehenden E-Mails.

Die erste Art besteht aus E-Mails mit besonderen Kategorien von personenbezogenen Daten, die in den meisten Organisationen insbesondere im Rahmen von per E-Mail verschickten Bewerbungsunterlagen anfallen dürften und aus denen ggfs. die Religionszugehörigkeit oder der Schwerbehindertenstatus hervorgehen. Für solche E-Mails sollte zum Schutz der Rechte und Freiheiten betroffener Personen eine besonders kurze Löschfrist gelten. Diese E-Mails sollten daher durch Mitarbeiter zum Zeitpunkt ihres Empfangs in einen entsprechenden Ordner im E-Mail-Postfach verschoben werden und eine automatisierte Löschregel für den Ordner aktiviert werden. Der Zeitraum, der für die Löschregel ausgewählt wird, sollte sich nach der spezifischen Aufbewahrungsfrist für die in dem Ordner enthaltenen Daten richten. Enthält der Ordner also Bewerbungen, so können diese i.d.R. sechs Monate nach Ende des Bewerbungsverfahrens gelöscht werden. Dementsprechend muss für die Festlegung des Löschzeitpunkts zunächst ermittelt werden, wie lange ein Bewerbungsverfahren von der Ausschreibung bis zum Besetzen einer Stelle bei dem Verantwortlichen andauert. Dauert ein Bewerbungsverfahren z.B. regelmäßig drei bzw. sechs Monate, so sollte die Löschregel des Ordners auf neun[6] bzw. zwölf[7] Monate eingestellt werden.

Die zweite Art sollte E-Mails betreffen, für die aufgrund ihres besonderen Inhalts längere Aufbewahrungsfristen gelten müssen, um schutzwürdige Interessen des Verantwortlichen berücksichtigen zu können, ohne dass durch die längere Aufbewahrungsfrist Rechte und Freiheiten betroffener Personen unangemessen eingeschränkt werden. Das wären etwa alle E-Mails, die eine patentrechtliche Relevanz haben. Diese E-Mails enthalten i.d.R. keine besonders schützenswerten personenbezogenen Daten, vielmehr sind die Angaben über Patentanmelder usw. „notwendiges Beiwerk" des Patentanmeldeverfahrens. Die E-Mails wären in einen Ordner zu verschieben, der eine entsprechend längere Aufbewahrung vorsieht. Für diesen Ordner sollte eine „Löscherinnerung" nach Ablauf des Zeitraums, in dem der Verantwortliche ein schutzwürdiges Interesse an der Aufbewahrung der Daten hat, gesetzt werden. Im Falle von Patentsachen könnte die Löscherinnerung bspw. nach 20 Jahren erfolgen, da Patente gem. § 16 PatG eine Gültigkeit von 20 Jahren ab dem Anmeldetag haben. Wird die Löscherinnerung ausgelöst, so wäre manuell zu prüfen, ob die E-Mails gelöscht werden können oder weiter aufbewahrt werden müssen (und die Löscherinnerung somit verlängert werden müsste), weil z.B. das Patent verlängert werden soll.

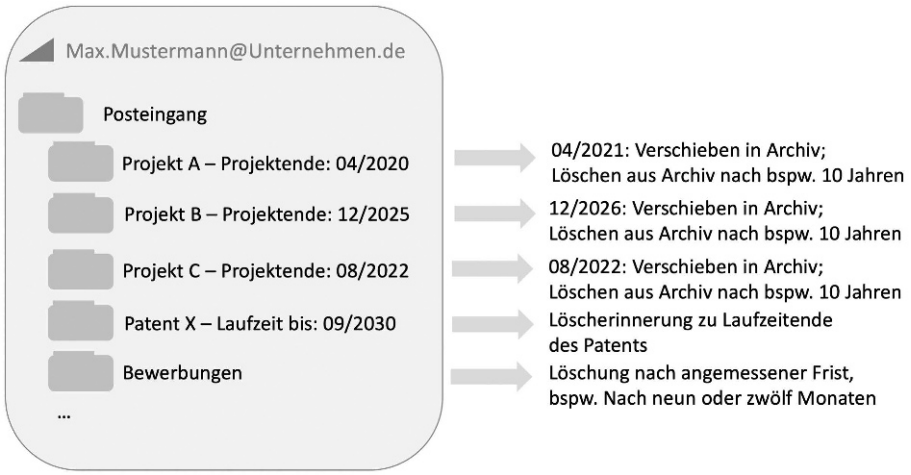
Die dritte Art betrifft alle anderen E-Mails, also insbesondere E-Mails, die jeglicher Projektkommunikation zuzuordnen sind. Für solche E-Mails sollte ein Unterordner je Projekt/Vorgangsreihe angelegt werden und den Namen des Projektes erhalten. Ausgehend von der Annahme, dass man im Nachgang eines Projektes/Vorgangs i.d.R. noch ein Jahr auf die E-Mails zugreifen können muss, um beispielsweise Informationen für Projektabschlussberichte zu extrahieren, sich die Notwendigkeit der Aufbewahrung von E-Mails ein Jahr nach Abschluss eines Projektes/Vorgangs jedoch i.d.R. auf gesetzliche Aufbewahrungspflichten beschränkt, könnte jeder Projektunterordner ein Jahr nach Projektende in ein separates Archiv verschoben werden und die E-Mails dort für den Zeitraum der längsten für den Verantwortlichen geltenden Aufbewahrungspflicht vorgehalten werden. Die längste

5 Die Anwendungsfälle der Arten 1 und 2 können bei jedem Verantwortlichen variieren und sind daher individuell zu ermitteln. Bewerbungsdaten und Patentsachen sind insofern nur Beispiele zur Veranschaulichung des Umsetzungsvorschlags.

6 Drei Monate Bewerbungsverfahren + sechs Monate Aufbewahrung nach Ende des Bewerbungsverfahrens.

7 Sechs Monate Bewerbungsverfahren + sechs Monate Aufbewahrung nach Ende des Bewerbungsverfahrens.

Abbildung 1: Umgang mit Löschvorgaben bei E-Mails



Aufbewahrungsfrist eines Verantwortlichen könnte sich z.B. aus dem Handels- und Steuerrecht ergeben und zehn Jahre betragen. Nach Ablauf der längsten für den Verantwortlichen einschlägigen Aufbewahrungsfrist könnten die Daten im Archiv automatisiert gelöscht werden.

Durch das Verschieben des Unterordners in ein Archiv wären die E-Mails im Wirkbetrieb nicht mehr verfügbar. Auf das Archiv sollte grundsätzlich kein Zugriffsrecht bestehen. Eine Ausnahme sollte lediglich für das Erfüllen gesetzlicher Aufbewahrungspflichten (und ggf. von Löschanträgen betroffener Personen) bestehen. Insofern wäre das Archiv mit einem Zugriffsschutz zu versehen, um es vor unbefugtem Zugriff zu schützen. Dies kann bspw. durch einen Passwortschutz in Verbindung mit einer verbindlichen Organisationsanweisung des Arbeitgebers, der das Zugriffsverbot und deren Ausnahmen regelt, technisch-organisatorisch umgesetzt werden. Ein weiterer Schutzmechanismus gegen unberechtigte/exzessive Zugriffe auf das Archiv könnte z.B. in der Pflicht bestehen, notwendige Zugriffe auf das Archiv zu dokumentieren. Zusätzlich kann auch eine automatische Protokollierung der Zugriffe hilfreich sein, um dem unberechtigten Zugriff entgegenzuwirken bzw. die Umsetzung des Zugriffsschutzes zu kontrollieren.

Die Aufbewahrung in den Archiven entzieht die Verarbeitung der E-Mails dem Wirkbetrieb und erschwert dadurch weitere potentielle Verarbeitungen. Die Archivlösung wirkt somit potenziellen Risiken für die Rechte und Freiheiten betroffener Personen entgegen, indem die Verarbeitung der Daten eingeschränkt wird, nachdem das Projekt/der Vorgang abgeschlossen ist, die E-Mails aber noch bis zum Ablauf der längsten Aufbewahrungspflicht im Archiv vorgehalten werden. Da durch die erste Art von E-Mails bereits besondere Kategorien personenbezogener Daten, deren Verarbeitung ggf. höhere Risiken für die Rechte und Freiheiten betroffener Personen mit sich bringt, herausgefiltert wurden, scheint der Schutzbedarf der verbleibenden personenbezogenen Daten in der dritten Art von E-Mails sowie der technisch-organisatorische Schutz auch unter pauschaler Anwendung der längsten für den Verantwortlichen geltenden Aufbewahrungspflicht angemessen. Hierbei ist auch das finanzielle Risiko des Verantwortlichen zu berücksichtigen, sofern bspw. steuerrechtlich aufzubewahrende E-Mails zu früh gelöscht würden. Das Risiko, dass Mitarbeiter bei der Kategorisierung eingehender Mails in bspw. „Bewerbungen", „Patentsachen" und „sonstige (Projekt-)Kommunikation" Fehler unterlaufen, kann hierbei – im Gegensatz zu der individuellen Festlegung von Löschzeitpunkten je E-Mail durch den Mitarbeiter – als gering eingestuft werden.

Im Ergebnis ist das hier beschriebene Modell zur Löschung von E-Mails sowohl geeignet als auch angemessen.

5 Ergänzende Maßnahmen

In Ergänzung zu dem vorgeschlagenen Lösungsweg „Archivieren & anschließendes Löschen von E-Mails" sind ggf. weitere technische und organisatorische Maßnahmen notwendig, die der Verantwortliche unternehmens- bzw. organisationsweit einführen sollte, um die Löschvorgaben der DSGVO umzusetzen.

5.1 Umgang mit Altbeständen

Das vorgestellte Verfahren ist vorwiegend dazu konzipiert, neu eingehende E-Mails systematisch in Unterordner zu verschieben und auf die einzelnen Unterordner pauschale Lösch- und Archivierungsregeln anzuwenden. Trotzdem kann das Verfahren auch zur Bereinigung des „E-Mail-Altbestandes" angewandt werden. Die Umsetzung würde nach dem gleichen Prinzip erfolgen, es müssten nach besten Kräften nur diejenigen E-Mails mit sensiblen Inhalten, bspw. Bewerbungsunterlagen, sowie E-Mails mit längeren Aufbewahrungsfristen, bspw. Patentsachen, herausgesucht werden und entsprechend der zuvor dargestellten Regeln gelöscht/weiter aufbewahrt werden. Der danach verbleibende Restbestand sollte in ein Archiv verschoben werden, welches dann ebenfalls nach zehn Jahren eine Löschung vorsieht. Sofern im Restbestand E-Mails enthalten sind, die älter sind als zehn Jahre, sollten diese gelöscht werden, unter der Voraussetzung, dass sie keine Patentsachen (oder ähnliche, schutzwürdige Angelegenheiten) betreffen.

5.2 Umgang mit E-Mail-Ausdrucken

In einigen Unternehmen und Forschungseinrichtungen werden besonders wichtige E-Mails ausgedruckt und in Papierakten aufgenommen – z.B. in Rechtsabteilungen, dem Einkauf oder in Reisestellen. Ist dies der Fall, könnte der Verantwortliche in einer Organisationsanweisung regeln, dass ausgedruckte E-Mails datenschutzkonform – also zugriffsgeschützt – aufzubewahren sind und spätestens analog zum E-Mail-Archiv datenschutzkonform vernichtet werden müssen. Nach DIN 66399 wären Ausdrucke von E-Mails demnach gemäß den Vorgaben des Sicherheitslevels 3,[8] sofern auf dem Ausdruck besondere Kategorien personenbezogener Daten enthalten sind ggf. sogar gemäß den Vorgaben des Sicherheitslevels 4[9] zu schreddern [3].

8 Sicherheitslevel 3: Fläche der Materialteilchen max. 320 mm² oder Breite des Streifens max. 2 mm bei unbegrenzter Seitenlänge.

9 Sicherheitslevel 4: Fläche der Materialteilchen max. 160 mm² und für gleichförmige Partikel eine max. Breite des Streifens von 6 mm.

5.3 Nachweis der Löschung

Der Verantwortliche muss darüber hinaus Maßnahmen zur Nachweisbarkeit der Löschung treffen. Insbesondere muss der Verantwortliche die technischen und organisatorischen Maßnahmen auf der prozessualen Ebene darlegen. Das bedeutet im Kontext der Löschung von E-Mails, dass die Vorgehensweise der Löschung in der Organisation nachvollziehbar beschrieben ist, etwa in Form eines Löschkonzepts oder im Verzeichnis der Verarbeitungstätigkeiten, das ohnehin – wenn möglich – die Löschfristen zu enthalten hat. Des Weiteren ist der Verantwortliche dazu angehalten, die konkrete Vorgehensweise der Datenlöschung an die entsprechenden Mitarbeiter zu kommunizieren und dies nachweisen zu können. Je nach Anwendungskontext und (sinnvollerweise) verfügbaren technisch-organisatorischen Möglichkeiten zur Umsetzung kann auch die Protokollierung von Löschvorgängen Teil der Nachweispflichten sein.

5.4 Löschregeln bei Auftragsverarbeitung

Sollte im Zusammenhang mit E-Mail-Anwendungen auf einen Auftragsverarbeiter zurückgegriffen werden, sind vertragliche Regelungen zur Löschung personenbezogener Daten nach Abschluss der Leistungserbringung durch den Auftragsverarbeiter gem. Art. 28 Abs. 3 S. 2 lit. g DSGVO verpflichtend zu treffen. Nach Beendigung der Auftragsverarbeitung sollte der Auftragsverarbeiter dem Verantwortlichen die Löschung sämtlicher Daten durch ein Löschprotokoll bzw. eine Löschbestätigung nachweisen. Diese Pflicht sollte ggf. explizit im Auftragsverarbeitungsvertrag festgeschrieben werden.

6 Fazit

In der betrieblichen Praxis ist die E-Mail eines der wichtigsten Kommunikationsmittel. Die in ihr enthaltenen personenbezogenen Daten unterliegen den allgemeinen datenschutzrechtlichen Löschvorgaben. Diese im Anwendungskontext „E-Mail" jedoch in geeigneter Weise und angemessen umzusetzen, stellt Verantwortliche nicht zuletzt aufgrund der schieren Masse an ein- und ausgehenden E-Mails vor eine große Herausforderung.

Geeignet und angemessen könnte insbesondere sein, die E-Mails je E-Mail-Postfach in drei Arten einzuordnen:

- E-Mails, die zum Schutz der betroffenen Personen nach besonders kurzer Zeit gelöscht werden müssen;
- E-Mails, die aus schutzwürdigen Interessen des Verantwortlichen besonders lange aufbewahrt werden müssen;
- alle anderen ein- und ausgehenden E-Mails, die ein Jahr nach Vorgangs-/Projektende in ein zugriffsgeschütztes Archiv verschoben werden sollten, für das als automatische Löschregel die längste für den Verantwortlichen relevante Aufbewahrungsfrist einzustellen wäre.

Für die ersten beiden Arten wären jeweils Unterordner im Mailpostfach zu erstellen und die jeweiligen Unterordner mit Löschregeln bzw. Löscherinnerungen zu versehen.

Darüber hinaus sollten u.a. der Umgang mit E-Mail-Altbeständen und E-Mail-Ausdrucken geregelt werden sowie der Nachweis der Löschung – u.a. durch das Anfertigen von Löschkonzepten und -protokollen – erbracht werden.

Literatur

[1] Aßmus, Ubbo, Datenschutzrechtliche Anforderungen an die E-Mail-Aufbewahrung im Unternehmen: Grenzen und Gestaltungsmöglichkeiten, Hamburg, 2014.

[2] Auernhammer, Herbert/ Eßer, Martin/ Kramer, Philipp/ von Lewinski, Kai, Auernhammer DSGVO BDSG, Köln, 2018.

[3] Deutsches Institut für Normung, DIN-Standard 66399-1, und DIN-Standard 66399-2, Berlin 2012.

[4] Gierschmann, Sibylle, Schlender, Katharina/ Stentzel, Rainer/ Veil, Winfried, Kommentar Datenschutz-Grundverordnung, Köln, 2018.

[5] Gola, Peter, DS-GVO Datenschutz- Grundverordnung VO (EU) 2016/ 679, München, 2. Auflage 2018.

[6] Gola, Peter/ Heckmann, Dirk, Bundesdatenschutzgesetz, München, 2019.

[7] Kühling, Jürgen/ Buchner, Benedikt, DS-GVO Datenschutz- Grundverordnung, München, 2018.

[8] Meyer, Jörg, Forensische Datenanalyse, Berlin, 2012.

[9] Müller-Glöge, Rudi/ Preis, Ulrich/ Schmidt, Ingrid, Erfurter Kommentar zum Arbeitsrecht, München, 2019.

[10] Plath, Kai- Uwe, BDSG/ DSGVO, Köln, 3. Auflage 2018.

[11] Reiners, Wilfried, E-Mail Compliance fordert E-Mail Richtlinie, DuD 2010, 630.