PSP
MÜNCHEN

White Paper

E-Mail-Archivierung und DSGVO

Autor: Dr. Axel-Michael Wagner

[Januar 2019]

ZUSAMMENFASSUNG

Jede Speicherung von E-Mails bringt die Verarbeitung personenbezogener Daten im Sinne des Datenschutzrechts mit sich, denn im Datenschutzrecht genügen das Empfangen und kürzeste (Zwischen-)Speicherzeiten, um von einer „Verarbeitung" personenbezogener Daten auszugehen. Mit dem Inkrafttreten der DSGVO stellen sich gerade bei elektronischer Post diverse Fragen von der Zulässigkeit einer Voll- oder Journalarchivierung unternehmensbezogener E-Mails bis hin zum Aussortieren des privaten E-Mailverkehrs. Das White Paper „E-Mail-Archivierung und DSGVO" zeigt auf, wann und warum Unternehmen bei automatischer E-Mail-Archivierung an rechtliche Grenzen stoßen und gibt Hilfestellungen für die Unternehmenspraxis.

Inhalt

Einleitung

Jedes Unternehmen, das E-Mails empfangen oder senden kann – also jedes –, speichert eingehende E-Mails. Entweder geschieht dies im Unternehmen selbst oder bei einem Dienstleister (Mailserverbetreiber), der die E-Mails dann wiederum zum Abruf durch die Mitarbeiter zur Verfügung stellt. Ab welcher Speicherdauer das „Speichern" begrifflich zum „Archivieren" wird (also das „Produktivsystem" zum „Archivsystem"), ist dabei datenschutzrechtlich irrelevant. Für das Datenschutzrecht genügen auch das Empfangen und kürzeste (Zwischen-)Speicherzeiten, um von einer „Verarbeitung" personenbezogener Daten auszugehen. Im Grundsatz ist das Datenschutzrecht auf sämtliche E-Mails im unternehmerischen Umfeld anwendbar, da diese personenbezogene Daten enthalten und „automatisiert" verarbeitet werden. E-Mails, die keine personenbezogenen Daten enthalten, sind zwar theoretisch denkbar, in der Praxis aber eine absolute Ausnahme: Reine Maschinen-zu-Maschinen-Kommunikation wird üblicherweise nicht über E-Mails abgewickelt.

Jede E-Mail-Verarbeitung bedeutet also rechtlich (unter anderem) die Verarbeitung personenbezogener Daten. Viele Unternehmen verarbeiten E-Mails aber nicht nur insoweit, als ihr Zweck dies unbedingt erforderlich machen würde, sondern schieben sämtliche ein- und ausgehenden E-Mails in (Langzeit-)Archive. Dies kann – ganz profan – eine Unterordnerstruktur in einem E-Mail-Programm wie Outlook sein, in die eingehende E-Mails eingeordnet und „nie" gelöscht werden. Dies können Backup-Mechanismen sein, die zu einer „endlosen Folge" von per Volltextsuche durchsuchbaren E-Mails führen (Journalarchivierung). Immer ausgefeilter werden demgegenüber die Möglichkeiten von Dokumentenmanagementsystemen, in denen Daten – also auch E-Mails – mit umfangreichen Index- bzw. Metadaten versehen und so besser auffindbar werden. Derartige Systeme können mit entsprechenden Filtern bzw. Eingrenzungen die Suche nach der sprichwörtlichen „Stecknadel im Heuhaufen" wesentlich vereinfachen.

Hinter diesen Archivierungsbestrebungen stehen im Wesentlichen drei Motive.

Erstens könnte man die Information ja irgendwann noch einmal im eigenen Interesse – zu möglicherweise noch gar nicht vorhersehbaren Zwecken – brauchen: „Wer Daten löscht, ist selbst dran schuld, wenn er sie später sucht und nicht mehr hat". Kosten spielen dabei keine erhebliche Rolle, denn Speicherplatz wird exponentiell günstiger. Die Spitze dieser Entwicklung ist „big data" bzw. der „data lake": Erst einmal möglichst viele Daten sammeln und dann sehen, was man mit ihnen noch so alles anstellen kann.

Zweitens gibt es insbesondere im Bereich des Steuerrechts immer weitergehende Vorgaben für Art und Dauer der Archivierung steuerlich relevanter Daten. Was alles „steuerlich relevant" ist, kann weder durch menschliche noch durch künstliche Intelligenz genau abgegrenzt werden, schon gar nicht zu überschaubaren Kosten. Deshalb ist die unveränderbare Archivierung von „allem" einfacher, denn dann muss nicht mit der Betriebsprüfung darüber diskutiert werden, ob man die Daten, die man nicht mehr hat, hätte haben müssen.

Und drittens schätzt jedes Unternehmen den Aufwand, Informationen im „Massendatenverkehr" inhaltlich zuverlässig zu klassifizieren und anhand dessen zu entscheiden, ob und wenn ja, wie lange diese in Archivsystemen aufbewahrt werden sollen, als unverhältnismäßig ein. Überdies geht mit jeder „händischen" Selektion von Daten anhand ihres Inhalts das Risiko der Fehleinschätzung einher, sei es aufgrund von Flüchtigkeitsfehlern oder „Subsumtionsmängeln" der hierfür eingesetzten Personen. Dieses Risiko kann bislang – und auch in naher Zukunft – auch durch den Einsatz „künstlicher Intelligenz" nicht ausgeschlossen werden, sodass es naheliegt und günstiger ist, sicherheitshalber sämtliche Korrespondenz aufzubewahren.

Jede Speicherung von E-Mails ist datenschutzrechtlich relevant!

Löschpflichten

Im Grundsatz ordnet die DSGVO an, dass personenbezogene Daten zu löschen sind, wenn sämtliche datenschutzrechtlichen „Behaltensgründe“ ausgefallen sind. Wann diese Löschpflicht vorliegt, wird nachfolgend im Einzelnen untersucht. Wichtig ist aber, dass die Löschpflicht, wenn sie einmal vorliegt, keiner Risikoabwägung unterliegt. Mit anderen Worten: Es kann nicht auf das Löschen verzichtet werden, weil es sich um keine „risikobehafteten“ Daten handelt oder nur sehr wenige Menschen und unter sehr einschränkenden Bedingungen darauf Zugriff haben. Außerdem bedeutet das Löschen digitaler Daten tatsächlich das Löschen der Daten, nicht nur das Sperren (Berechtigungsentzug). Dies schließt die Löschung von Backup-Daten ein, wobei hier von den Aufsichtsbehörden eine „Karenzzeit“ hinsichtlich revolvierender Backups von bis zu einem Jahr angedeutet wurde.

Die einzige zulässige Alternative zum Löschen ist übrigens die Anonymisierung, denn diese nimmt den Daten ihren Charakter als personenbezogen. Eine Anonymisierung kann übrigens auch dadurch erreicht werden, dass die Daten so aufwendig verschlüsselt werden, dass sie ohne den Schlüssel („Zuordnungsregel“) nicht mehr mit zumutbarem Aufwand entschlüsselt werden können, und der Schlüssel selbst „weggeworfen“ wird. Möglicherweise – aber das ist bislang „unerforscht“ – kann der Schlüssel anstatt des „Wegwerfens“ auch an einen vertrauenswürdigen Dritten weitergegeben werden (Notar o. ä.), der diesen zwar unter keinen Umständen an das Unternehmen, unter bestimmten Umständen aber in einem gerichtlichen Verfahren herausgeben darf, damit dann mit den entschlüsselten Daten ein Beweis geführt werden kann. Bedauerlicherweise könnte die – orakelhafte – Entscheidung des Europäischen Gerichtshofs zu dynamischen IP-Adressen einer solchen „Treuhandlösung“ im Wege stehen, denn eine Staatsanwaltschaft könnte den Schlüssel beschlagnahmen und das Ergebnis der Entschlüsselung könnte dann dem Unternehmen (als Geschädigtem) im Rahmen einer Akteneinsicht wieder zufließen. Damit wäre die Anonymisierung nurmehr eine Pseudonymisierung und daher nicht geeignet, den personenbezogenen Daten ihren Personenbezug zu nehmen.

Löschen heißt Löschen, inklusive Backups!

Zweckverbrauch

Aus datenschutzrechtlicher Perspektive ist die erste Grenze der Speicherdauer der Zweck der Datenverarbeitung. Wenn man sich per E-Mail mit einem Kollegen (lediglich) zu einer Besprechung vereinbart hat und der Termin stattgefunden hat, ist der Zweck „verbraucht". Nun ist aber der datenschutzrechtliche „Zweckverbrauch" einer E-Mail – ebenso wie schon die Ermittlung des Zwecks selbst – kein mathematisch exakt bestimmbarer Zeitpunkt. Ein erster Anhaltspunkt ist allenfalls der Umstand, dass E-Mails in der Praxis häufig bewusst „gelöscht" (oder „weggeklickt") werden, sobald man ihren Inhalt intellektuell „irgendwie" verarbeitet hat. Regelmäßig kann jedoch nicht davon ausgegangen werden, dass das „Wegklicken" einer E-Mail gleichbedeutend mit einem datenschutzrechtlichen Zweckverbrauch ist. Das beginnt schon damit, dass man häufig in seinen (vor kurzem) gelöschten E-Mails nach Informationen sucht, d. h. diese haben weiterhin „irgendeine" Relevanz – ob diese Relevanz datenschutzrechtlich erheblich ist, ist eine Frage, die nur für den konkreten Einzelfall beantwortet werden kann. Wenn nun sämtliche Mitarbeiter in sämtlichen Unternehmen bei Erhalt, Versendung oder beim „Wegklicken" einer E-Mail zusätzlich darüber sinnieren müssten, wann der Zweck der E-Mail datenschutzrechtlich „verbraucht" wurde, müsste man wohl – obwohl das Datenschutzrecht dies eigentlich fordert – von einer neuen Generation von „bullshit jobs" sprechen.

Eine Löschung wegen Zweckverbrauchs (bzw. Zweckfortfalls) lässt sich demnach schlecht im Massengeschäft realisieren. Die „künstliche Intelligenz", sozusagen der heilige Gral der Digitalisierung, ist noch nicht hinreichend einsatzbereit, der Einsatz von (geschultem!) Personal zum „Grübeln über den Einzelfall" nicht zumutbar. Es bleibt deshalb in diesem Bereich – wie auch in anderen Bereichen, dazu noch unten – die Definition eines Rasters bzw. von Löschkategorien, in die Daten automatisiert, teilautomatisiert oder händisch einsortiert werden und bei denen die Gefahr besteht, dass ein Datensatz „durchs Raster fällt".

Der Zweckverbrauch als erster „Löschpunkt" lässt sich allgemein nicht bestimmen.

Durchsetzung von Rechtsansprüchen oder Verteidigung gegen solche

Selbst im einfachen Fall der Vereinbarung zwischen Kollegen zu einer Besprechung kann es Jahre später in einem Ermittlungsverfahren von entscheidender Bedeutung sein, ob an diesem Tag die Besprechung stattgefunden hat oder nicht – und der E-Mail-Verkehr kann dabei ein wichtiges Beweismittel sein. Die zweite Grenze der Speicherdauer scheinen damit Verjährungsfristen zu sein. Solange noch ein Rechtsanspruch geltend gemacht bzw. eine Ordnungswidrigkeit oder Straftat verfolgt werden kann, liegt es – mit einem gewissen Restrisiko, denn Information kann be- und entlastend sein – im eigenen Interesse, Daten aufzubewahren. Das spricht für eine Archivierung.

Ob die DSGVO diesen „Schlenker" mit der Folge einer weitgehenden Außerkraftsetzung grundlegender Datenschutzprinzipien (Zweckbindung, Datenminimierung, Speicherbegrenzung) mitgeht, ist mehr als offen. Nach herkömmlicher Lesart gibt es zwei voneinander unabhängige Löschverpflichtungen des Verantwortlichen, eine „aus sich selbst heraus" (antragsunabhängige „Speicherbegrenzung") und eine als Folge eines Rechts auf Löschung seitens des Betroffenen (antragsabhängige Löschpflicht). Schon für die Frage, ob für beide Löschverpflichtungen dieselben Grenzen gelten, gibt es keine eindeutige Antwort. Zumindest dann aber, wenn ein Betroffener die Löschung „seiner" Daten (die Beweismittel sein können) verlangt, will die DSGVO verhindern, dass dies nur zu dem Zweck geschieht, die Rechtsverfolgung zu erschweren. Daher gilt die Löschverpflichtung solange nicht, als die weitere Speicherung „erforderlich ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen". Liest man dies wörtlich, dann müsste zumindest dann, wenn im Zeitpunkt des Zweckverbrauchs „weit und breit" keine Geltendmachung oder Ausübung eines Rechtsanspruchs bzw. keine Verteidigung gegen einen solchen in Sicht ist, gelöscht werden. Die Bandbreite liegt also zwischen „bereits konkret geltend gemacht" (dann müsste schon ein Verfahren anhängig sein) und „könnte theoretisch noch geltend gemacht werden" (dann würde die abstrakte Gefahr genügen, innerhalb der Verjährungsfrist in Anspruch genommen zu werden). Die DSGVO sagt dazu ausdrücklich nichts. Die Kommentarliteratur zu dieser Frage spricht häufig von einer Abwägung zwischen Löschung und Inanspruchnahmerisiko, also davon, dass (nur) ein „absehbares Verfahren gegen die betroffene Person selbst" den Löschungsanspruch ausschließt, dass „eine bloß abstrakte Möglichkeit einer rechtlichen Auseinandersetzung" nicht genügt oder dass „Auseinandersetzungen anstehen oder mit hinreichender Wahrscheinlichkeit zu erwarten" sein müssen. Vereinzelt gibt es aber auch Juristen, die demgegenüber in einer laufenden Verjährungsfrist das Maß aller Dinge

sehen. Das mag bei kürzeren Fristen wie der Verjährungsfrist für vertragliche Gewährleistungsansprüche (in der Regel zwei Jahre) noch leichter „verdaulich" sein als die zivilrechtlichen Maximalverjährungsfristen von 30 Jahren, welche die meisten Datenschützer schon „vom Ergebnis her" wohl nicht mehr mitgehen werden. Schöner wäre es in jedem Fall gewesen, wenn der Gesetzgeber sich über diese in der Praxis nicht unerhebliche Frage mehr Gedanken gemacht und diese (im Gesetzestext) niedergelegt hätte. Vermutlich hat sich aber der Gesetzgeber – wie so oft – gar keine weiteren Gedanken dazu gemacht.

Rechtfertigungsgrundlage einer „anlasslosen", längerfristigen Speicherung personenbezogener Daten kann daher die Durchsetzung von Rechtsansprüchen bzw. die Verteidigung gegen ebensolche kaum sein. Dieses Verbot der präventiven Beweismittelsicherstellung mutet vielen Unternehmen (und auch Juristen) absurd an und lädt daher zu „zivilem Ungehorsam" ein. Es würde auch viele Complianceuntersuchungen nutzlos machen, die einige Zeit nach der „Tat" versuchen sollen, diese anhand möglichst objektiver Beweisquellen aufzuklären.

Es ist unklar, wie lange personenbezogene Daten mit dem Argument einer drohenden rechtlichen Auseinandersetzung (inkl. Ermittlungsverfahren) zu „präventiven Beweiszwecken" gespeichert werden dürfen. Bestehen keine Anhaltspunkte, dass eine solche Auseinandersetzung droht, ist die Berufung auf eine Berechtigung zur weiteren Speicherung aus diesem Grund riskant.

Das rettende Ufer: Die Aufbewahrungspflichten

Damit rückt der herkömmlich für die Archivierung angeführte „Grund zur Nicht-Löschung“ in den Fokus: Die Berufung auf Aufbewahrungspflichten. Der Gesetzgeber neigt – unabhängig von der DSGVO – vermehrt dazu, den Unternehmen Aufbewahrungspflichten aufzugeben. Da der Staat dem Bürger bzw. Unternehmen im Verwaltungs- und im Strafverfahren ein Fehlverhalten nachweisen muss, ist es wichtig, mögliche Beweismittel hierfür unter teils drakonischen Strafandrohungen vorhalten zu lassen, gewissermaßen als „Preis“ für diese Beweislast. Die DSGVO bezeichnet Aufbewahrungspflichten auch nicht als solche, sondern man muss diese in den sperrigen Passus „Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert“ hineinlesen.

Die Aufgabenstellung besteht hier also „nur“ darin, die einzelnen gesetzlichen Pflichten zur Datenaufbewahrung zu identifizieren und die E-Mails den so gebildeten „Löschklassen“ zuzuordnen. Das entscheidende Problem ist dabei jedoch die Granularität. Versucht man, die DSGVO sehr „feingranular“ anzuwenden, stellen sich im Rahmen des „Grübelns über den Einzelfall“ viele Fragen. Auf der anderen Seite der Skala steht eine hochgranulare Analyse jeder einzelnen E-Mail: Wer hat an wen geschrieben? Über welche identifizierbare Person wird in der E-Mail geschrieben? Enthält die E-Mail besondere Kategorien personenbezogener Daten? Welche Aufbewahrungsfristen gelten konkret für ihren spezifischen Inhalt? Welche Einwilligungen, welche Interessenbekundungen haben die involvierten Personen hinsichtlich der Speicherung eventuell bereits erteilt und sind diese noch wirksam? Es liegt auf der Hand, dass diese „Subsumtionsarbeit“ durch Personal unzumutbar, durch künstliche Intelligenz zumindest derzeit nicht lösbar ist.

Auf der einen Seite der Skala steht die Einschätzung, dass es irgendeine Frist gibt, die aus irgendeinem Grund für „sämtliche E-Mails“ anwendbar ist. Dies kann von der IT einfach umgesetzt werden: Nach Ablauf dieser Zeit werden die E-Mails gelöscht und entsprechend der Backup-Zyklen verschwinden die E-Mails irgendwann auch aus den Backups. Dafür gibt es im Wesentlichen zwei Kandidaten: § 147 AO und § 257 HGB.

Bevor diese Kandidaten vertieft erörtert werden, ist allerdings klarzustellen, dass bei Nicht-Löschung personenbezogener Daten wegen Aufbewahrungspflichten, obwohl diese „eigentlich“ datenschutzrechtlich hätten gelöscht werden müssen, der Zweck der Datenspeicherung auf die Aufbewahrungspflicht beschränkt ist. Die Daten dürfen also nur gespeichert und – von engen Ausnahmen abgesehen – nicht (mehr) zu den ursprünglichen, zwischenzeitlich

aber entfallenen Zwecken verwendet werden (z. B. nicht mehr für Direktmarketing bzw. die Kontaktaufnahme). Eine fortlaufende Speicherung wegen steuerlicher Archivierungspflichten ist daher alleine geeignet, eine spätere Einsichtnahme in die Daten durch den Betriebsprüfer oder den Steuerberater, allenfalls noch durch die unternehmenseigene Steuerabteilung, zu legitimieren. Eine Verwendung der Daten zu „big data"-Zwecken würde den Daten, die eigentlich schon längst hätten gelöscht werden müssen, einen neuen Zweck unterschieben. Ebenso wäre die Verwendung dieser Daten zu Zwecken der Durchsetzung von Rechtsansprüchen bzw. zur Verteidigung gegen ebensolche wohl datenschutzrechtlich bedenklich, wenn zu dem Zeitpunkt, zu dem sie „eigentlich" hätten gelöscht werden müssen, von der Geltendmachung dieser konkreten Rechtsansprüche „weit und breit" nichts zu sehen war.

Nach der Theorie wird die Löschung dergestalt operationalisiert, dass Löschfristen für einzelne Datenarten ermittelt und zu Löschklassen zusammengefasst werden, auf die dann Löschregeln angewendet werden. Dies ergibt sich z. B. aus der DIN 66398 – „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten". Wann nun was zu löschen ist, ergibt sich auch aus dieser Norm nicht; es geht dabei nur um ein Verfahren, mit dem diese Erkenntnis gewonnen und angewandt werden kann. Man kann sich dabei leicht vorstellen, dass das nicht gerade sehr schlanke deutsche Recht vielfältige Aufbewahrungsfristen vorgibt – alleine im Bereich der Beschäftigtendaten wurden bereits mehrere dutzend Regelungen identifiziert, die für einzelne Datenarten gelten.

Es lässt sich also resümieren, dass einerseits die Ermittlung der geltenden Aufbewahrungsvorschriften, andererseits die Atomisierung und Einteilung „unternehmenstypischer" Daten in Datenarten, auf die diese Aufbewahrungsvorschriften Anwendung finden, der Kern eines mustergültigen Löschkonzepts sind. Bei dieser Form des „Mappings" lassen sich herkömmlich zumindest drei Granularitätsebenen unterscheiden: Akte, Dokument und Einzeldatum. Man kann eine Personalakte als Personalakte behandeln und löschen, man kann auf Dokumentebene die einzelne Arbeitsunfähigkeitsbescheinigung als Einzeldokument behandeln und löschen, und man kann auf Einzeldatumsebene eine einzelne Angabe in der Arbeitsunfähigkeitsbescheinigung als Einzeldatum behandeln und löschen (schwärzen). Ähnlich kann man E-Mail-Verkehre inkl. ihrer Attachments eher grob- oder feingranular analysieren.

Aufbewahrungspflichten „durchbrechen“ die datenschutzrechtlichen Löschpflichten. Die Daten dürfen dann aber nur zu den Zwecken der jeweiligen Aufbewahrungspflicht weiter gespeichert werden. Die Identifikation von Aufbewahrungsfristen und die Kategorisierung von Datenbeständen anhand der Aufbewahrungsfristen ist in der Praxis aufwendig.

PSP
MÜNCHEN

Steuerliche und handelsrechtliche Zehn-Jahres-Aufbewahrungspflichten

Eine Zehn-Jahres-Aufbewahrungspflicht gilt nach § 147 AO für „Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen", „Buchungsbelege" und bestimmte Zollunterlagen. Mit „Büchern" sind hier „nicht nur Handelsbücher, sondern auch alle anderen Geschäftsbücher, z. B. Haupt-, Grund-, Nebenbücher, Kontokorrentbücher oder Kontenkarten usw., die für steuerliche Zwecke geführt werden" gemeint. Buchungsbelege hingegen umfassen „Rechnungen, Lieferscheine, Quittungen, Auftragszettel, Warenbestandsaufnahmen, Bankauszüge, Betriebskostenabrechnungen, Bewertungsunterlagen, Buchungsanweisungen, Gehaltslisten, Kassenberichte, Portokassenbücher, Prozessakten". Für „Rechnungen" (sowohl die Eingangsrechnungen als auch jeweils ein „Doppel" der Ausgangsrechnungen) schreibt § 14b UStG die Zehn-Jahres-Archivierung noch einmal gesondert vor. Es ist leicht ersichtlich, dass eine Vielzahl der E-Mails, die in und zwischen Unternehmen versendet werden, gleichwohl nicht bzw. nicht ohne Weiteres diesen Kategorien zugeordnet werden kann. Nur am Rande soll darauf hingewiesen werden, dass sich die Zehn-Jahres-Frist verlängert, wenn vor ihrem Ablauf eine Betriebsprüfung stattfindet (sog. „Ablaufhemmung"), was entsprechend (durch eine sog. „legal hold notice") operationalisiert werden muss.

Nach § 257 HGB gilt eine Zehn-Jahres-Aufbewahrungspflicht für „Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen" sowie für „Buchungsbelege". Im hiesigen Kontext der E-Mail-Archivierung besteht also eine weitreichende Überschneidung zu den Objekten der oben dargestellten steuerlichen Aufbewahrungspflicht des § 147 AO.

Sämtliche dieser Fristen beginnen erst am jeweiligen Kalenderjahresende der Erstellung bzw. des Empfangs des entsprechenden Dokuments, d. h. sie können bis zu (knapp) elf Jahre betragen.

Einige, aber bei weitem nicht alle E-Mails im unternehmerischen Umfeld werden unter die steuerlichen und handelsrechtlichen Zehn-Jahres-Aufbewahrungspflichten fallen.

Steuerliche und handelsrechtliche Sechs-Jahres-Aufbewahrungspflichten

Daneben gelten nach den genannten Vorschriften der AO und des HGB sechsjährige Aufbewahrungsfristen u. a. für „Handels- und Geschäftsbriefe". Handelsbriefe sind Schriftstücke (auch in elektronischer Form), welche die Vorbereitung, den Abschluss, die Durchführung oder die Rückgängigmachung von Handelsgeschäften zum Gegenstand haben. Geschäftsbriefe sind Mitteilungen im geschäftlichen Bereich in Textform, die im Namen des Unternehmens verfasst und individuell adressiert sind. Aber: Es muss sich um eine im weitesten Sinn rechtsgeschäftserhebliche Mitteilung handeln, also etwa um Angebote, Vertragserklärungen, Mahnungen, Mängelrügen, Kündigungen oder „Bestellscheine". Hingegen fehlt es „Grußkarten", Hinweisen auf Firmenjubiläen, Schließungen und Öffnungen, unverbindlichem PR-Verkehr mit zufriedenen oder unzufriedenen Kunden sowie Werbung an einer solche Qualität.

Daraus ergibt sich, dass viele – aber bei weitem nicht alle – E-Mails unter die Sechs-Jahres-Aufbewahrungspflicht fallen werden. Im Einzelfall kann die Abgrenzung auch durchaus rechtlich zweifelhaft sein. Dies beginnt schon bei Rechnungen, die als Attachment zu einer E-Mail gesendet werden. Die Rechnung selbst muss für zehn Jahre (s. o.), die E-Mail – da sie selbst keine Rechnung, sondern „nur" einen Handels- und Geschäftsbrief darstellt – nur für sechs Jahre aufbewahrt werden. Auch die GoBD („*Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff*") der Finanzverwaltung sehen vor, dass eine E-Mail, die nur als „Umschlag" für eine als Attachment beigefügte Rechnung fungiert, aus rein steuerlichen Gründen nicht archiviert werden muss. Dennoch können sich auch aus der E-Mail rechnungserhebliche Informationen (etwa der Hinweis auf eine Rabattaktion) ergeben, sodass zusätzlich die E-Mail selbst – als Folge steuerlicher „Sippenhaft" – gemeinsam mit dem Rechnungs-Attachment für die längere Frist aufbewahrungspflichtig sein dürfte. Um daher „auf der sicheren Seite zu sein", wenn der Betriebsprüfer die E-Mail auch nach Ablauf von sechs Jahren sehen möchte, aber auch wegen des Aufwands der Trennung von E-Mail und Attachment, bewahren viele Unternehmen beides gleichermaßen für die längere Aufbewahrungsfrist auf. Auch bei E-Mails, die im Wesentlichen „PR-Charakter" haben, aber dennoch beiläufig an eine bestehende rechtliche Beziehung anknüpfen, kann deren rechtliche „Doppelqualifizierung" die Einordnung erschweren. Vor dem Hintergrund des Handels- und Steuerrechts wird man eher dazu neigen, im Zweifel „auf der sicheren Seite" zu sein und eher mehr als weniger zu archivieren. Vor dem Hintergrund des Datenschutzrechts müsste man

jedoch – platt gesagt – dazu neigen, im Zweifel „auf der sicheren Seite“ zu sein und eher weniger als mehr zu archivieren.

Viele, aber bei weitem nicht alle E-Mails im unternehmerischen Umfeld fallen unter die steuerlichen und handelsrechtlichen Sechs-Jahres-Aufbewahrungspflichten.

Vertragliche Aufbewahrungsfristen

Der deutsche Gesetzgeber hat die Beschränkung auf „gesetzliche“ Aufbewahrungspflichten dadurch aufgeweicht, dass nach dem neuen Bundesdatenschutzgesetz in Ergänzung zur DSGVO auch satzungsgemäße oder vertragliche Aufbewahrungsfristen der (datenschutzrechtlichen) Löschung entgegenstehen können. Der Verantwortliche, der sich satzungsmäßig verankerten oder vereinbarten Verpflichtungen gegenübersieht, soll vor einem Konflikt mit der Löschpflicht bewahrt werden. Dem liegt der – allerdings eher antiquierte – Gedanke zugrunde, eine (passive) „Aufbewahrung“ mit entsprechender Sperrung weitergehender Verwendung sei datenschutzrechtlich „nicht so schlimm“ wie eine weitere produktive (aktive) Verwendung und könne daher auch durch (in Satzungen bzw. Gesellschaftsverträgen von Handels- oder Kapitalgesellschaften bzw. Vereinen oder anderweit) lediglich vereinbarte Aufbewahrungsfristen legitimiert werden. Spätestens seitdem weitreichende Recherchemöglichkeiten auch in Archivsystemen gegeben sind und „big data“-Auswertungen auf sämtliche Daten zugreifen, die „irgendwo“ greifbar sind, erscheinen diese „hinübergeretteten“ Spezialregelungen des „alten“ Datenschutzrechts (d. h. vor der DSGVO) aus der Zeit gefallen. Die Vereinbarkeit dieser deutschen Gesetzgebung mit der DSGVO wird jedoch bislang nicht in Zweifel gezogen.

Die Regelung wirft allerdings wieder einmal mehr Fragen auf, als sie beantwortet. Kann einerseits einfach in jede Satzung jedes Unternehmens eine „satzungsmäßige“ Aufbewahrungspflicht für personenbezogene Daten bis zum sprichwörtlichen „Sankt Nimmerleinstag“ aufgenommen werden? Das klingt sehr nach „juristischem Abrakadabra“; immerhin wird hier die Pflichtenkollision des Verantwortlichen, die von der Regelung gelöst werden soll, erst mutwillig geschaffen. Ein Anhaltspunkt dafür allerdings, dass nur „Altregelungen“ vor Inkrafttreten der DSGVO die weitere Aufbewahrung legitimieren, findet sich im Gesetz (und auch in der Gesetzesbegründung) nicht. Und wo dürfen andererseits „vertragliche Aufbewahrungsfristen“ vorgesehen werden, nur in Verträgen zwischen dem Verantwortlichen und dem Betroffenen oder auch in Verträgen zwischen dem Verantwortlichen und (irgendwelchen) Dritten? Erste Kommentierungen beschränken dies – ohne Anhaltspunkt im Gesetzestext (oder in der Gesetzesbegründung) – auf vertragliche Bindungen mit der betroffenen Person selbst. Das ist zwar verständlich, denn ansonsten könnte in „irgendeinem“ Vertrag des Verantwortlichen mit „irgendeinem“ Dritten die Aufbewahrung sämtlicher personenbezogener Daten für einen unbefristeten Zeitraum vereinbart werden. Mit dieser – an sich sinnvollen – Einschränkung hätte es allerdings dieser gesetzlichen Regelung gar nicht bedurft: Ist in

einem Vertrag zwischen Verantwortlichem und Betroffenem geregelt, dass die Daten für einen bestimmten Zeitraum aufzubewahren sind, dann ist die Aufbewahrung schon zu eben diesem Vertragszweck „erforderlich".

Es gibt also – wie so oft – „Unschärfen" und intuitive Zweifel an der Sinnhaftigkeit der gesetzlichen Regelung, die auf den ersten Blick wie die sprichwörtliche „eierlegende Wollmilchsau" der E-Mail-Archivierung aussieht, auch weil sie von einem Widerspruch/Widerruf des Betroffenen unabhängig ist. Unabhängig davon dürfte allerdings die Aufnahme einer sinngemäßen Bestimmung in die Satzung eines Unternehmens, dass „sämtliche Daten, welche die Gesellschaft im Rahmen ihrer Tätigkeit verarbeitet, einschließlich personenbezogener Daten, für einen Zeitraum von [x] Jahren aufzubewahren sind", nicht schaden können. Es bleibt abzuwarten, bis die ersten juristischen Stimmen laut werden, dass „das so nicht geht".

Die Aufnahme von Aufbewahrungspflichten des Verantwortlichen in dessen Satzung sowie in Verträgen – sowohl mit dem Betroffenen als auch mit Dritten – stellt datenschutzrechtlich ein vom Gesetz legitimiertes Argument für eine entsprechende Aufbewahrung auch nach Zweckverbrauch und gegen den Willen des Betroffenen dar, dessen juristischer Bestand allerdings unklar ist.

Folge dieser Regelung ist übrigens, dass die Daten nicht gelöscht werden müssen, sondern nur „eingeschränkt verarbeitet" werden dürfen. Einschränkung der Verarbeitung bedeutet, dass die Daten „nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden" dürfen.

Wichtig ist in diesem Zusammenhang auch, dass satzungsgemäße oder vertragliche Aufbewahrungspflichten nicht die datenschutzrechtliche Legitimationsgrundlage für die Verarbeitung ersetzen, sondern nur die Löschpflicht einschränken können. Wer also Daten gar nicht „haben darf", sprich ohne datenschutzrechtliche Legitimationsgrundlage besitzt, darf diese auch nicht bei Bestehen einer satzungsgemäßen oder vertraglichen Aufbewahrungspflicht aufbewahren.

Speicherung von Direktmarketingkommunikation

Sieht man einmal von satzungs- und vereinbarungsgemäßen Aufbewahrungsfristen ab, die theoretisch inhaltlich sämtliche personenbezogenen Daten umfassen könnten, machen zumindest die oben erörterten einschlägigen gesetzlichen Aufbewahrungspflichten eine inhaltliche Kategorisierung der Korrespondenz in Handels- und Geschäftsbriefe und „sonstige" Korrespondenz notwendig. Der wohl (weitaus) überwiegende Teil der „sonstigen" im Unternehmen anfallenden Kommunikation dürfte zu „Direktmarketingzwecken" erfolgen – so würde man „PR-Kommunikation" im Datenschutzrecht nennen. Damit stellt sich die Frage, ob es einen außerhalb der steuer- und handelsrechtlichen Aufbewahrungsfristen liegenden Grund geben könnte, solche Direktmarketingkommunikation längerfristig zu speichern. Auf das Thema der privaten E-Mails der Beschäftigen wird noch weiter unten eingegangen. Es wird sich zeigen, dass diese Thematik – die eigentlich nur die „Residualgröße" der nicht von gesetzlichen Aufbewahrungspflichten erfassten E-Mails betrifft – sehr grundsätzliche Fragen des Datenschutzrechts berührt.

Im Kern geht es hier darum, dass der Mitarbeiter eines Unternehmens an einen Mitarbeiter eines anderen Unternehmens irgendeine Form von Marketingkommunikation sendet. Das muss keine Werbung im engeren Sinne sein, sondern der Begriff Direktmarketing umfasst auch soziale, karitative, politische und ähnliche Kommunikationszwecke. Die entsprechende E-Mail wird typischerweise in beiden Unternehmen gespeichert, d. h. sowohl beim Sender als auch beim Empfänger. Damit gibt es zwei „Betroffene", jeweils einen „unternehmenseigenen" und einen „unternehmensfremden", und – unabhängig voneinander – zwei Verantwortliche, die die Direktmarketingkommunikation mit den personenbezogenen Daten der Betroffenen übermitteln und speichern. Wenn es also um die Legitimationsgrundlage für die Archivierung (Speicherung) geht, muss in Bezug auf beide Betroffene eine entsprechende Grundlage vorhanden sein, und idealerweise darüber hinaus auch für Drittbetroffene, über die in der Kommunikation ggf. gesprochen wird.

Fallgestaltung: *Der Leiter einer Einkaufsabteilung eines Unternehmens, der während seiner Unternehmenszugehörigkeit mit viel Direktmarketing(Werbe-)kommunikation für Waren und Dienstleistungen „überschwemmt" wurde (und zum Teil natürlich auch darauf geantwortet hat), scheidet aus dem Unternehmen aus. Die Kommunikation wurde stets über sein Unternehmens-E-Mail-Postfach abgewickelt. Er widerspricht gegenüber seinem ehemaligen Arbeitgeber sowie gegenüber sämtlichen Unternehmen, die ihm im Laufe der Zeit (ggf. auch in Beantwortung seiner eigenen E-Mails) derartige Kommunikation gesandt haben, etwaigen Interessenabwägungen mit Direktmarketinginteressen. Er fordert sowohl von seinem ehemaligen Arbeitgeber als auch von den dritten Unternehmen die Löschung der gesamten historischen Korrespondenz.*

Intuitiv würden beide Unternehmen in Bezug auf die (historischen) Kommunikationen sagen, dass es hier um „unternehmensbezogene" Kommunikationsdaten geht, die nur insoweit personenbezogen sind, als sie unternehmensbezogene Kontaktdaten des Mitarbeiters beinhalten, nicht aber „persönliche" Daten des Mitarbeiters. Das Problem dabei ist nur: Das Datenschutzrecht unterscheidet nicht zwischen diesen Kategorien. Auch die unternehmensbezogenen Kontaktdaten, die in den E-Mails enthalten sind (Absender, Empfänger, Aliasname, E-Mail-Signatur etc.), sind ebenso wie die verfassten Inhalte selbst personenbezogen.

Soweit es im Beispiel um den Leiter der Einkaufsabteilung, also um den „unternehmenseigenen" Kommunikationsteilnehmer, geht, fällt auf der Suche nach einer datenschutzrechtlichen Legitimationsgrundlage ein berechtigtes betriebliches Interesse des Arbeitgebers ins Auge, derartige Kommunikationen aufzubewahren, um die Historie der Kommunikation zwischen Unternehmen (Kunden, Lieferanten, Dienstleistern) später nachvollziehen zu können – unabhängig von Aufbewahrungspflichten. Es ist wahrscheinlich, dass das Interesse des ehemaligen Mitarbeiters, dass sämtliche unternehmensbezogene historische Kommunikation von ihm gelöscht wird, gegenüber diesem berechtigten Interesse des ehemaligen Arbeitgebers zurücktreten muss, solange es sich nicht um „sensible" Daten, sondern „nur" um unternehmensbezogene Kontaktdaten und Kommunikation handelt. Die entscheidende Frage ist allenfalls, wie lange die Verarbeitung dieser personenbezogenen Daten für die Zwecke des betrieblichen Interesses „erforderlich" ist. Eine „endlose" Speicherung wird datenschutzrechtlich nicht „erforderlich" sein. 2010 – also lange vor Einführung der DSGVO – hat das Landgericht München einmal in Bezug auf die Speicherdauer von zu Werbezwecken eingesetzten Kontaktdaten geurteilt, dass sich solche Daten ohne zwischenzeitliche Kontaktaufnahme bzw. Reaktion seitens des Betroffenen nach 17 Monaten „verbraucht" hätten. Wenn das Landgericht München damals geahnt hätte, dass diese Entscheidung zwischen-

zeitlich – in Ermangelung gesetzgeberischer Vorgaben und höchstrichterlicher Rechtsprechung – von den Datenschutzbehörden zum „Maß aller Dinge“ selbst unter der DSGVO erhoben wurde...

Unabhängig von der Frage aber, wie lange die DSGVO im Kontext der Archivierung unter dem Blickwinkel der Interessenabwägung die Archivierung derartiger Kommunikation zulassen würde, handelt es sich bei dieser Argumentation jedenfalls um einen „Pyrrhussieg“. Denn der ehemalige Mitarbeiter kann dieser – wie jeder anderen – Interessenabwägung widersprechen und dann dürfen die betroffenen Daten zunächst nicht mehr verarbeitet (also auch gespeichert) werden, „es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“ (Art. 21 Abs. 1 DSGVO). So stark wird aber das Interesse des ehemaligen Arbeitgebers nicht sein. Erteilt der Mitarbeiter bei seinem Ausscheiden eine Einwilligung zur weiteren Speicherung, kann er diese Einwilligung ebenfalls jederzeit widerrufen. Im oben dargestellten Fall würde in der Forderung nach Löschung natürlich auch ein Widerspruch gegen die Interessenabwägung (und die weitere Verarbeitung auf dieser Grundlage) liegen.

Damit rückt die Frage in den Vordergrund, ob nicht das (beendete) Anstellungsverhältnis noch eine datenschutzrechtliche Legitimationsbasis für die Archivierung unternehmensbezogener Kommunikation sein kann. Schließlich stehen die vom ehemaligen Mitarbeiter verfassten Kommunikationen im Zusammenhang mit dessen Beschäftigungsverhältnis. Es ist „erforderlich“, dass ein Einkaufsleiter nach außen hin das Unternehmen repräsentiert, damit er seiner Funktion im Unternehmen gerecht werden kann; der Mitarbeiter erfüllt damit seine Pflicht zur Ableistung der vereinbarten Arbeit, das Unternehmen seine Pflicht, dem Mitarbeiter Arbeit zuzuweisen. Kann nun aber datenschutzrechtlich argumentiert werden, dass die Speicherung unternehmensbezogener Direktmarketingkommunikation – mit personenbezogenen Daten – „erforderlich“ ist für die „Durchführung eines Beschäftigungsverhältnisses“? Dies würde im Übrigen auch Brief- und Faxverkehr betreffen, aber letztlich auch außerhalb des Bereichs „Direktmarketing“ internen Schriftverkehr innerhalb des Unternehmens wie Arbeitsanweisungen und Ähnliches. Ein Mitarbeiter hinterlässt schließlich während seiner Unternehmenszugehörigkeit einen „bleibenden Eindruck“ in Form von Datenspuren im Unternehmen. Wenn man die bisherige Kommentarliteratur zu diesem Thema wälzt, die solche „historischen Kommunikationsdaten“ des Mitarbeiters kaum explizit thematisiert, ist es eher unwahrscheinlich, dass das Anstellungsverhältnis eine hinreichende datenschutzrechtliche Legitimation darstellt. Es wäre auch völlig unklar, wie lange das (bereits

beendete) Anstellungsverhältnis überhaupt eine solche Legitimationsgrundlage darstellen könnte.

Im Hinblick auf die personenbezogenen Daten des „unternehmensfremden" Mitarbeiters stellt Direktmarketing durchaus ein „berechtigtes Interesse" des verarbeitenden Verantwortlichen im Sinne der datenschutzrechtlichen Legitimationsgrundlage „Interessenabwägung" dar, dem im Regelfall kein überwiegendes Interesse des Betroffenen entgegensteht. Geht man davon aus, dass Einwilligung und berechtigtes Interesse in keinem Rangverhältnis zueinander stehen, kann eine Verarbeitung von personenbezogenen Daten zumindest in Form von unternehmensbezogenen Kontaktdaten (Name, betriebliche E-Mail-Adresse, Unternehmenszugehörigkeit, Telefondurchwahl etc.) – also „Niedrigrisikodaten" – zu Direktmarketingzwecken im sog. „opt out"-Wege begründet werden. Im Grundsatz ist die Verarbeitung dieser personenbezogenen Daten zu Direktmarketingzwecken bis zum Widerruf („opt out") seitens des Betroffenen möglich. Dabei stellt sich allerdings generell die Folgefrage, ob sich das Direktmarketinginteresse nicht durch Zeitablauf irgendwann „verbraucht", sodass die entsprechenden Kontaktdaten auch ohne Widerruf zu löschen sind, wenn keine Reaktion (mehr) vonseiten des Angesprochenen auf die Kontaktaufnahme erfolgt. Was in diesem Kontext meist nicht erörtert wird, ist, inwieweit das berechtigte Direktmarketinginteresse nicht nur das Speichern und Verwenden (zur Kommunikation) der Stammdaten des Betroffenen legitimiert, sondern auch die Speicherung (Archivierung) historischer „Direktmarketingkommunikation" (einschließlich von – auch nur internen – Aufzeichnungen über den Verlauf des Kontakts). Davon unabhängig besteht natürlich auch hier die Möglichkeit, der Interessenabwägung jederzeit zu widersprechen.

Sowohl aus der Perspektive des „unternehmenseigenen" Mitarbeiters als auch im Hinblick auf die Daten des „unternehmensfremden" Mitarbeiters liegt eine datenschutzrechtliche Legitimationsgrundlage wohl nur bis zu einem Widerruf vor. Das ist misslich, denn dies führt dazu, dass im Widerrufsfalle sämtliche entsprechenden Kommunikationen unmittelbar „aus dem Archiv entfernt", d. h. endgültig gelöscht (oder anonymisiert) werden müssen. Der entsprechende „Filteraufwand" ist immens, sodass es sich anbietet, die entsprechenden Inhalte schon bei der Versendung bzw. beim Empfang zu kategorisieren.

Natürlich ist dieses Ergebnis für das Unternehmen kontraintuitiv. Man würde als Unternehmen schon in Frage stellen, ob es überhaupt einer datenschutzrechtlichen Interessenabwägung gegen ein „privates" Interesse des Betroffenen bedarf, weil es hier um unternehmensbezogene Kommunikation geht. Das Direktmarketinginteresse des marketingbetreibenden Unternehmens richtet sich meist gar nicht auf die angesprochene Person als solche, sondern auf das (Ziel-)Unternehmen selbst, welches zwangsläufig durch natürliche Personen repräsentiert wird. Die „unternehmensbezogene" Direktmarketingkommunikation enthält lediglich unternehmensbezogene Kontaktdaten natürlicher Personen und wird nicht zum Zweck des Direktmarketings gegenüber dieser natürlichen Person (sondern gegenüber dem dahinterstehenden Unternehmen) ausgetauscht. Kurz gesagt handelt es sich um „Unternehmenskommunikation". Bedauerlicherweise unterscheidet die DSGVO aber nicht zwischen „unternehmensbezogenen" und „privaten" Daten, sondern ausschließlich zwischen „personenbezogenen" und „nicht-personenbezogenen" Daten.

Ein weiteres Thema in diesem Zusammenhang, das hier ausgeklammert wird, sind die datenschutzrechtlichen Pflichthinweise, die dem Betroffenen zur Verfügung zu stellen sind. Dies gilt für die Archivierung der Kommunikation „unternehmenseigener" Mitarbeiter ebenso wie für die Kommunikation „unternehmensfremder" Dritter.

Werden in einer Direktmarketingkommunikation personenbezogene Daten Dritter ausgetauscht, können sich zusätzliche Fragestellungen ergeben. Wenn etwa der Mitarbeiter eines Cateringunternehmens den Einkaufsleiter im obigen Beispiel anschreibt und ihm eine Bezugsadresse für besonderen Wein für die nächste Betriebsfeier nennt, werden personenbezogene Daten des Mitarbeiters des Weinhändlers übermittelt. Ob der Einkaufsleiter – gleich, ob er diese unternehmensbezogenen Kontaktdaten des Weinhändlermitarbeiters „verwendet" oder nicht – dem Weinhändlermitarbeiter unmittelbar datenschutzrechtliche Pflichthinweise zur Verfügung stellen muss, ist unklar. Es lässt sich rechtfertigen, dass diesbezüglich keine Pflicht besteht (wohl aber möglicherweise eine Pflicht des Cateringunternehmens, die Weitergabe der Kontaktdaten als Zweckänderung anzuzeigen). Würde nun der Mitarbeiter des Weinhändlers ausscheiden und diesen auffordern, sämtliche Daten über sich zu löschen (außer für Zwecke gesetzlicher Aufbewahrungspflichten), müsste der Weinhändler das Cateringunternehmen und das Cateringunternehmen den Einkaufsleiter benachrichtigen, und das Unternehmen des Einkaufsleiters müsste dann die betroffenen Kommunikationen (ebenso wie die Stammdaten des Weinhändlermitarbeiters, wenn diese z. B. in die EDV des Unternehmens eingepflegt wurden) zu löschen.

Private Daten als Teil der zu archivierenden Daten

Schon innerhalb derselben E-Mail lässt sich oft nicht zwischen unternehmensbezogener und privater Kommunikation unterscheiden. Die Formel „Dienst ist Dienst und Schnaps ist Schnaps“ ist anachronistisch. Man spricht vom „work-life blend“, vom nahtlosen Ineinanderübergehen von Privatleben und Job. Eine E-Mail fragt erst nach dem Besuch beim Fußballspiel mit dem „Sohnemann“, nach dem letzten Urlaub in Tirol, um dann zum geschäftlichen Anliegen überzuleiten.

Nach herkömmlicher Auffassung wird ein Arbeitgeber, der seinen Arbeitnehmern – ob durch betriebliche Übung (auch entgegen einer anderslautenden Absprache) oder durch Vereinbarung – die Unternehmens-EDV für den Empfang und die Versendung privater E-Mails zur Verfügung stellt, zum sogenannten Telekommunikationsanbieter. Damit ist das „Fernmeldegeheimnis“ auf die privaten E-Mail-Verkehre anwendbar, und zwar auch nach dem Zeitpunkt, zu dem die E-Mail im Postfach des Mitarbeiters „abgeliefert“ wurde, wenn der Arbeitgeber auch dann noch in der Lage ist, jederzeit auf die betreffenden E-Mails zuzugreifen (insbesondere auch durch Archivierung) und der Arbeitnehmer keine technische Möglichkeit hat, eine Weitergabe durch den Arbeitgeber an fremde Personen (inkl. andere Arbeitnehmer) zu verhindern. Der Eingriff in das Fernmeldegeheimnis, das in diesem Fall der standardmäßigen Archivierung entgegensteht, ist zunächst einmal kein Thema des Datenschutzrechts. Aber natürlich stellt die Archivierung der privaten E-Mail durch den Arbeitgeber auch eine Verarbeitung personenbezogener Daten nach der DSGVO dar. Neuste Stimmen behaupten sogar, dass ausschließlich die DSGVO – auch im Zusammenhang mit dem Telekommunikationsvorgang bzw. mit dem Fernmeldegeheimnis – anwendbar ist.

Das Archivieren von privatem E-Mail-Verkehr von Mitarbeitern verstößt (wohl) gegen das Fernmeldegeheimnis. Dies gilt nur dann nicht, wenn dem Mitarbeiter die Verwendung des betrieblichen E-Mail-Postfachs vertraglich verboten wurde und die Einhaltung des Verbots durch den Arbeitgeber stichprobenmäßig immer wieder kontrolliert wird, denn dann ist der Arbeitgeber kein „Diensteanbieter“ und muss auch nicht mit privaten E-Mail-Verkehren rechnen.

Der Betroffene kann aber – neben der datenschutzrechtlichen Einwilligung in die Archivierung – in den Eingriff in das Fernmeldegeheimnis einwilligen. Eine freiwillige Einwilligung

zu Beginn des Beschäftigungsverhältnisses erscheint im Grundsatz – bei transparenter Information – möglich, weil der Arbeitnehmer durch die private Nutzbarkeit des E-Mail-Accounts ein „Mehr“ (im Verhältnis zu dem, was ihm der Arbeitgeber eigentlich schuldet) erhält und frei entscheiden kann, ob er dieses „Mehr“ mit dem Makel der automatischen Archivierung nutzen möchte oder (gar) nicht. In erster Näherung erscheint daher ein Ausfiltern privater E-Mails vor der Archivierung nicht notwendig zu sein, da durch Einwilligung eine entsprechende Legitimationsgrundlage geschaffen werden kann.

Was dabei allerdings oft vergessen wird, ist, dass nicht nur die Einwilligung des eigenen Mitarbeiters bei der Archivierung privater E-Mails erforderlich ist, sondern auch die des dritten Kommunikationspartners. Das Fernmeldegeheimnis schützt auch den Kommunikationsteilnehmer „auf der anderen Seite der Leitung“, der daneben auch (ebenso wie der kommunizierende Mitarbeiter) „Betroffener“ im Sinne des Datenschutzrechts ist. Der Arbeitnehmer kann nicht für seinen Kommunikationspartner auf dessen Rechte verzichten und jener wird – in aller Regel – keine (eigene) Einwilligung zum Eingriff in das Fernmeldegeheimnis erklären. Zweifelhaft ist daneben auch aus datenschutzrechtlicher Sicht, ob im Verhältnis zu diesem (externen) Kommunikationsteilnehmer ein berechtigtes Interesse im datenschutzrechtlichen Sinne gerade des Arbeitgebers seines (unternehmensinternen) Kommunikationspartners besteht, seine E-Mail-Korrespondenz dauerhaft zu archivieren. Schließlich kann schon die Archivierung privater E-Mails im Verhältnis zum eigenen Mitarbeiter kaum ein berechtigtes Interesse vorweisen, sodass der Arbeitgeber auf eine Einwilligung zur Archivierung (mit entsprechenden unternehmensinternen Zugriffsbeschränkungen) angewiesen ist.

Möglicherweise könnte man in Bezug auf das Fernmeldegeheimnis eine stillschweigende Einwilligung daraus folgern, dass ein externer Kommunikationspartner, der an eine unternehmensbezogene E-Mail-Adresse schreibt, wissen kann (muss?), dass Unternehmen E-Mails standardmäßig archivieren – und ggf. ansonsten auf eine rein private E-Mail-Adresse zurückgreifen bzw. diese erfragen muss. Als Einwilligung im datenschutzrechtlichen Sinne kann dies dagegen kaum einzustufen sein, da eine datenschutzrechtliche Einwilligung „informiert“ sein muss, d. h. ihr muss eine von der DSGVO vorgegebene Aufklärung, u. a. über die Möglichkeit und Wirkungen eines Widerrufs, vorangehen. Möglicherweise kann gleichwohl das Senden einer E-Mail an eine unternehmensbezogene E-Mail-Adresse datenschutzrechtlich immerhin dazu führen, dass eine Interessenabwägung mit dem Archivierungsinteresse des Arbeitgebers seines Kommunikationspartners zugunsten des Arbeitgebers ausgeht. Gegen die verminderte Schutzbedürftigkeit eines Absenders einer E-Mail an eine unternehmensbezogene E-Mail-Adresse spricht aber, dass in vielen Fällen E-Mail-Programme in der

Empfängerzeile nicht die „technische“ E-Mail-Adresse des Empfängers („peter.mueller@unternehmen.de“), sondern lediglich einen Aliasnamen („Peter Müller“) anzeigen. Daher wird es in vielen Fällen für den externen Kommunikationsteilnehmer nicht ohne Weiteres ersichtlich sein, dass er an eine Unternehmensadresse schreibt.

Nur ein vom Mitarbeiter selbst per Hand hinsichtlich der privaten E-Mail-Korrespondenz „vorgefilterter“ Posteingang kann damit rechtlich hinreichend sicher Gegenstand einer laufenden bzw. automatischen Archivierung sein. Auch eine Anweisung an den Mitarbeiter, für jeden privaten E-Mail-Kontakt automatisierte Regeln anzulegen, die entsprechend ein- und ausgehende E-Mails vor der Archivierung in einen privaten Ordner verschieben, dürfte nicht ausreichend sein, weil damit der erstmalige Empfang einer privaten E-Mail von einer bislang nicht von den Regeln erfassten Adresse unter die Archivierung fallen würde. Solange also der Mitarbeiter – aus welchem Grund auch immer (Krankheit, Urlaub, etc.) – nicht aussortieren kann, darf der Posteingang nicht archiviert werden und es darf auch sonst kein Zugriff des Arbeitgebers auf den Posteingang stattfinden.

Ergebnis

Eine automatische E-Mail-Archivierung der von einem Unternehmen empfangenen und gesendeten E-Mails stößt demnach an drei Grenzen:

- Widerspricht der Mitarbeiter (oder der betroffene Dritte) der Interessenabwägung, die einer Speicherung der mit seinen personenbezogenen Daten „durchsetzten" E-Mail-Kommunikation zugrunde liegt, müssen die entsprechenden Kommunikationen umgehend gelöscht werden, es sei denn, gesetzliche Aufbewahrungspflichten bestehen noch fort. Möglicherweise können auch satzungsmäßige und vertragliche Aufbewahrungspflichten dazu führen, dass die entsprechenden Kommunikationen weiter aufbewahrt (d. h. gegen sonstige Verwendung gesperrt) werden dürfen.
- Für unternehmensbezogene Kommunikationen, die keine Direktmarketingkommunikationen sind, finden – im Einzelnen unterschiedliche – gesetzliche Aufbewahrungsfristen Anwendung. Dies bedeutet, dass die E-Mail-Kommunikationen bei der Archivierung entsprechend der Aufbewahrungsfristen (wohl „von Hand") zu kategorisieren sind, denn wenn ein Widerspruch des betroffenen Mitarbeiters gegen die Interessenabwägung erhoben wird, kennzeichnen diese Aufbewahrungsfristen die „Höchstspeicherfristen". Wie hoch die „Höchstspeicherfrist" im Bereich der Direktmarketingkommunikationen sind, wenn kein Widerspruch erhoben wird, ist offen.
- Private E-Mails muss – abgesehen von der Sondersituation effektiv verbotener Nutzung des betrieblichen E-Mail-Accounts für private Kommunikation – der betroffene Mitarbeiter anhand von automatisierten Regeln oder „von Hand" aussortieren. Diese dürfen nicht mit archiviert werden.

Da heutzutage die Verwendung betrieblicher E-Mail-Accounts für private Zwecke meist – zumindest im Wege einer betrieblichen Übung entgegen entsprechender Regelungen in Anstellungsverträgen – geduldet wird, ist eine inhaltliche Aussortierung zumindest insoweit notwendig und eine Archivierung sämtlicher Korrespondenz („automatische Journalarchivierung") scheidet aus. Eine Archivierung sämtlicher unternehmensbezogener (d. h. nichtprivater) E-Mail-Korrespondenz ohne weitere Kategorisierung für einen definierten Zeitraum kann unabhängig von dieser „Vorfilterung" höchstens dann stattfinden, wenn man sich erfolgreich auf den rechtlich bislang nicht weiter vertieft diskutierten Ansatz der „satzungsmäßigen oder vertraglichen Aufbewahrungspflichten" berufen könnte. Ansonsten müssen die Daten im Rahmen der Archivierung von Hand danach kategorisiert werden, ob sie bei Vorliegen eines Widerspruchs durch eine bestimmte Person zu löschen sind bzw. welche gesetzliche Aufbewahrungsfrist zur Anwendung kommt.

Experten-Kontakt

Dr. Axel-Michael Wagner
Rechtsanwalt

E-Mail: a.wagner@psp.eu

Über PSP

Peters, Schönberger & Partner (PSP) zählt mit einer über 35-jährigen, erfolgreichen Unternehmenshistorie zu den renommiertesten mittelständischen Kanzleien in Deutschland. Als Steuerberater, Wirtschaftsprüfer und Rechtsanwälte unterstützen wir Sie bei wichtigen Entscheidungen und begleiten Sie bei deren Umsetzung. Zu unseren Mandanten zählen mittelständische Unternehmen, Familienunternehmen, vermögende Privatpersonen und Private Equity-Gesellschaften, die den Wunsch nach einer interdisziplinären und individuellen Beratung haben. Sie finden in uns einen professionellen, verlässlichen und durchsetzungsstarken Partner, der mit Leidenschaft Ihre rechtlichen und steuerlichen Interessen vertritt und auch die klassischen Aufgaben der Wirtschaftsprüfer übernimmt. Das PSP-Family Office unterstützt Sie zudem bei der Vermögensstrukturierung und verfügt über ausgewiesene Expertise in Nachfolge-, Stiftungs- und Immobilienfragen.

PETERS, SCHÖNBERGER & PARTNER
RECHTSANWÄLTE
WIRTSCHAFTSPRÜFER
STEUERBERATER
www.psp.eu