DSGVO – 11/2020 – Daten löschen in komplexen Systemlandschaften

DSGVO – 11/2020 – Daten löschen in komplexen Systemlandschaften

[expand title="mehr lesen…"]

Daten löschen in komplexen Systemlandschaften

Ballast abwerfen

Frank Heisel

Viele Unternehmen setzen das in der DSGVO geforderte Löschen obsoleter Daten entweder gar nicht oder nur unzureichend um. Da sich die Datenschutzaufsichtsbehörden in jüngster Zeit verstärkt für das Thema interessieren, müssen Firmen umdenken.

-tract

- Das datenschutzkonforme Löschen personenbezogener Informationen in verteilten Systemen ist eine anspruchsvolle Aufgabe, denn es gibt meist zahllose Abhängigkeiten zwischen den Daten.
- Dabei müssen die Verantwortlichen nicht nur rechtliche,

sondern auch viele technische Aspekte berücksichtigen.
- Bislang haben viele Unternehmen in dieser Hinsicht wenig getan. DSGVO, bissige Datenschutzbehörden und hohe Bußgelder zwingen sie nun zum Umdenken.

Personenbezogene Daten lassen sich in einem einzelnen System noch recht einfach löschen. In komplexen, heterogenen IT-Welten sieht die Sache anders aus. Hier gilt es, die Integrität, Verfügbarkeit und Konsistenz der Informationen nicht durch übereiltes Hantieren in den Datenbeständen zu gefährden.

Art. 17 Abs. 1 DSGVO räumt einem Betroffenen beim Vorliegen bestimmter Gründe das Recht ein, etwa die Betreiber eines Onlineshops dazu aufzufordern, seine persönlichen Daten unverzüglich aus den Systemen zu entfernen. Das anlassbezogene Löschen muss beispielsweise bei Widerruf einer erteilten Einwilligung erfolgen [Art. 17 Abs. 1 lit. b) DSGVO] oder bei - einem erfolgreichen Widerspruch gegen die Verarbeitung [Art. 17 Abs. 1 lit. c) DSGVO]. Der Artikel 17 regelt das sogenannte Recht auf Vergessenwerden.

In diesem Fall ergreift der Betroffene die Initiative. Um seinen Wunsch zu erfüllen, muss das Unternehmen einen Prozess implementiert haben, der das sofortige Prüfen der Anfrage einleitet. Dieser Prozess erfasst alle zugehörigen Datensätze, die über mehrere Systeme verteilt sein können. Nach der Überprüfung, ob und welche Daten gelöscht werden können, startet die zuständige Fachabteilung den Prozess manuell. Falls die Entwickler eine Löschfunktion eingerichtet haben, sollte man sie natürlich verwenden. Eine solche einfache Löschung funktioniert allerdings nur bei Systemen, die keine oder nur wenige Schnittstellen zu vor- und nachgelagerten Rechnern haben.

Das anlasslose Löschen verlangt das Entfernen von Daten, ohne dass jemand eine explizite Anfrage stellt. Diese Pflicht ergibt sich aus Art. 17 Abs. 1 lit. a) DSGVO. Danach müssen

Unternehmen personenbezogene Daten löschen, wenn der Zweck der Verarbeitung entfällt und keine Gründe gemäß Art. 17 Abs. 3 DSGVO dagegensprechen.

Die Aufgabe besteht nun darin, Löschfristen für einzelne Datensätze und -felder festzulegen, Löschregeln zu definieren und sie regelmäßig anzuwenden. Die Bereinigungsfrequenz dürfte sich in der Regel an den Aufbewahrungsfristen orientieren – je kürzer sie sind, desto höher die Rate der Wiederholungen. Bei wenigen und einfach strukturierten Daten lässt sich dieser Vorgang vergleichsweise einfach umsetzen, indem man einzelne Skripte zeitgesteuert ausführt oder manuell eingreift. Im Verbund mit anderen Systemen und verteilter Ablage der Daten kann das Löschen dagegen nur als Gesamtkonzept funktionieren, da ein ungeregelter Datenfluss zwischen den Systemen gelöschte Daten mit der nächsten Übertragung wieder einspielen kann.

Daten liegen überall verstreut

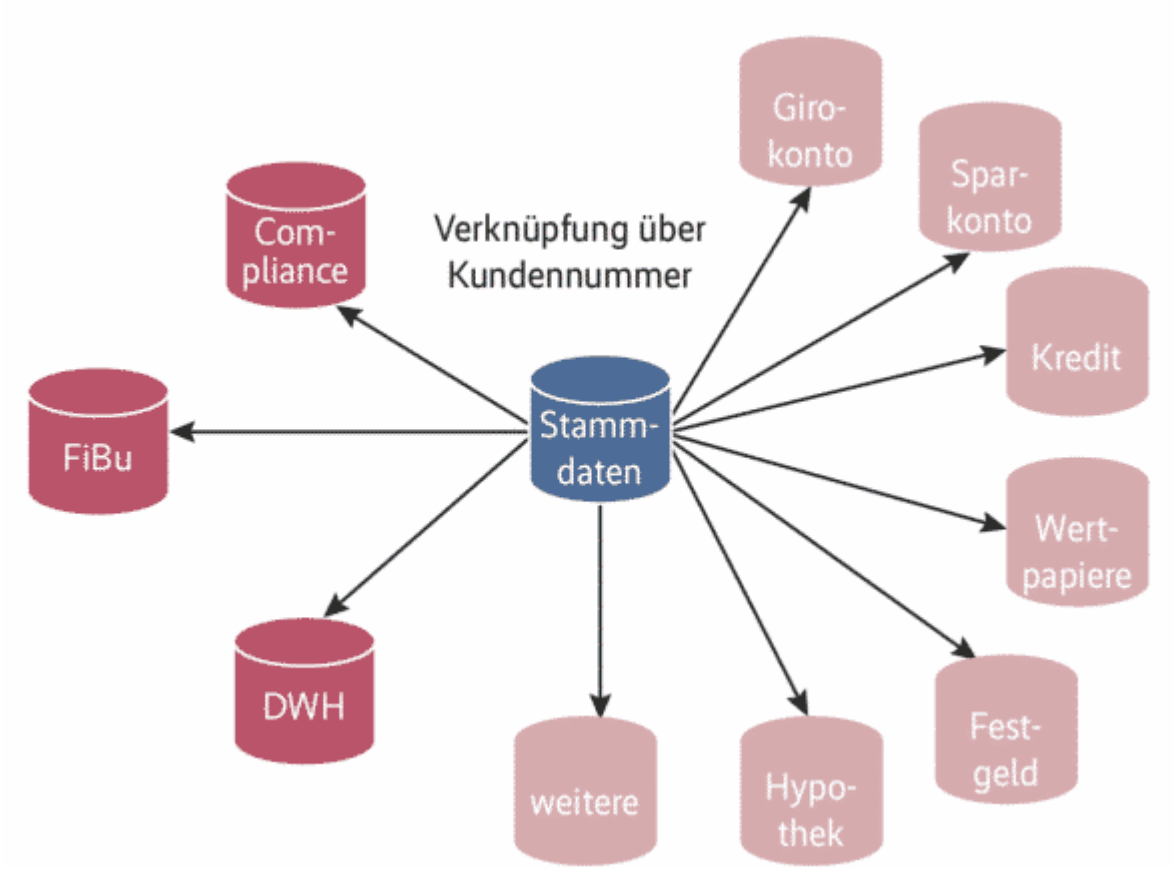
In größeren Organisationen besteht die IT-Landschaft gewöhnlich aus zahlreichen heterogen organisierten Anwendungen. Personenbezogene Daten werden zu verschiedenen Zwecken in vielen Datenbanken mehrfach oder verteilt gespeichert. Und nicht nur in den Produktivsystemen: Auch Entwicklungs- und Testumgebungen arbeiten oft damit.

In einem Webshop beispielsweise liefert der Kunde mindestens Name und Anschrift ab. Die Rechnungen werden als PDF gespeichert, per E-Mail versendet und an nachgelagerte Applikationen wie die Finanzbuchhaltung weitergereicht. Der Webshop will meist mehr wissen. Rechnungen müssen jedoch nur die in § 14 Abs. 4 UStG genannten Informationen enthalten. Alle erhobenen Daten landen normalerweise in einem CRM-System oder in einem Data Warehouse. Das Löschen einzelner Einträge muss daher in verschiedenen Systemen zu unterschiedlichen Zeitpunkten erfolgen.

Der Umfang der gespeicherten Daten verdient ebenfalls

Beachtung. Shop- oder CRM-Anwendungen erfassen außer dem Namen weitere Daten wie Kundennummer, Lieferanschrift, Rechnungsanschrift, Telefonnummer und E-Mail. Diese Daten sind notwendig, um die Bestellung zu bearbeiten, etwa um die Lieferung durch eine Spedition zu veranlassen und den Versand per E-Mail anzukündigen. Nach erfolgreicher Zustellung braucht man einiges davon zur Erfüllung des Vertrags jedoch nicht mehr. So sind für das Erstellen der Rechnung neben den Informationen zu den gelieferten Waren oder Leistungen lediglich der Name und die Anschrift des Empfängers, nicht jedoch die E-Mail-Adresse oder Telefonnummer erforderlich. Dafür entfällt dann der Verarbeitungszweck.

Komplexe Systeme verbinden die personenbezogenen Daten beispielsweise über ein Merkmal wie die Kundennummer (Abbildung 1). Die eigentlichen Daten liegen in der Stammdatenbank, alle anderen Systeme greifen lediglich über die Verknüpfung darauf zu. Zudem existieren viele Schnittstellen für den Datenaustausch. Bei einer Analyse des Datenflusses gehören alle Schnittstellen, über die personenbezogene Informationen laufen, in die Betrachtung. Wesentlichen Einfluss auf das Einsetzen einer datenschutzkonformen Löschung haben Faktoren wie der Umfang der personenbezogenen Daten, die Häufigkeit der Übertragung und die Art der Schnittstelle.



So etwa sieht die Systemlandschaft in einer Bank aus. Jedes Datenhaltungssystem speichert nur Teile eines kompletten Datensatzes. Löschen ist hier kompliziert (Abb. 1).

Akribische Untersuchungen sind notwendig

Die Fachabteilungen müssen für jede Schnittstelle zunächst erheben und dokumentieren, welche Daten sie wohin übermitteln. Entscheidend ist dabei, ob sie ausschließlich über ein systemweit eindeutiges Merkmal wie die Kundennummer verknüpft werden oder ob weitere Parameter im Spiel sind. Hier sollte man im Sinne einer guten „Privacy by Design“ darauf achten, dass nur notwendige Daten fließen. Bei Ausgangsrechnungen wäre es ausreichend, lediglich den Namen und die Anschrift des Rechnungsempfängers zu übertragen, nicht jedoch die weiteren Kontaktdaten.

Ein weiterer Aspekt ist die Häufigkeit der Übermittlung. Die meisten Schnittstellen dürften regelmäßig Daten erhalten und weitergeben. Falls das empfangende System eigene autonome Löschroutinen anbietet, müssen Übermittlungs- und

Löschfrequenz aufeinander abgestimmt sein, da es sonst vorkommen kann, dass Daten erneut übertragen werden und jemand sie im Zielsystem wieder löschen muss. Bei der Implementierung von Löschprozessen spielt daher die Art der Schnittstelle eine entscheidende Rolle.

Werden die Daten in Dateien verschickt, muss sichergestellt sein, dass auf dem abgebenden System oder einem eventuell zwischengeschalteten Fileserver keine Kopien verbleiben, da der Verarbeitungszweck nun erfüllt ist. Gegebenenfalls benötigt der Fileserver ein eigenes Löschkonzept, und er darf nicht als Backup oder Archiv missbraucht werden.

Eine Möglichkeit, Abhängigkeiten zu berücksichtigen, bieten zentrale Löschsysteme, die ihre Arbeit über alle angeschlossenen Systeme koordinieren und dafür sorgen, dass keine Daten verschwinden, die anderweitig noch benötigt werden. Man spricht in solchen Fällen von einer Orchestrierung der Löschung. Es gibt einige kommerzielle Produkte, etwa das Modul SAP ILM für die SAP-Welt, eine Alternative dazu namens - Cronos von der gleichnamigen Unternehmensberatung aus Münster und das universal einsetzbare Customer Data Deletion Management (CDMS) von Impetus.

Die zentrale Löschinstanz sammelt von allen Systemen die personenbezogenen Daten ein und hält sie in einer eigenen Datenbank. Die Löschregeln informieren bei Bedarf die Systemverantwortlichen über zu löschende Datensätze. Administratoren können dann das Löschen manuell oder automatisiert anstoßen und einen Nachweis an das zentrale Löschsystem schicken, das diesen archiviert. Hier angesiedelte Regeln sollten das unkontrollierte Löschen in den betroffenen Ablageorten verhindern. So lässt sich beispielsweise sicherstellen, dass der Stammdatensatz eines Kunden, der noch laufende Verträge hat, erst dann freigegeben wird, wenn alle Verträge beendet und die jeweiligen Aufbewahrungsfristen ausgelaufen sind.

Weiterer Vorteil einer zentralen Instanz: Unternehmen können sich bei einer Anfrage schnell einen Überblick darüber verschaffen, ob und welche Informationen zu dem Betroffenen vorliegen. Das Löschen lässt sich bei gesetzlichen Aufbewahrungsfristen mit einer entsprechenden Regel unterdrücken.

Manchmal müssen Daten verweilen

In bestimmten Situationen muss das Löschen grundsätzlich verhindert werden. Als Beispiel seien hier eine laufende Betriebsprüfung oder ein andauernder Rechtsstreit genannt. Bei einer Betriebsprüfung müssen die Daten bis zum Abschluss vorliegen. Hier bietet es sich an, die Frist zu verlängern. Relevante Daten zur Rechnungslegung liegen oft in Jahresarchiven, deren Löschung sich aussetzen lässt. Sie muss nach Abschluss der Prüfung manuell angestoßen werden. In jedem Fall sollte der verantwortliche Fachbereich vor dem Auslösen der regulären Löschung über den Vorgang mitbestimmen. Um nicht zu viele Daten auszunehmen, ist eine genaue Prüfung der Systeme und Daten notwendig.

Während eines Rechtsstreits müssen die benötigten Daten ebenfalls zur Verfügung stehen. In diesem Fall sollte die Rechtsabteilung die Fälle, deren Daten nicht gelöscht werden sollen, an den für das Löschen verantwortlichen Fachbereich übermitteln. Der nimmt die betroffenen Daten von der Löschung aus und entfernt sie nach Abschluss des Verfahrens einzeln. Alternativ bietet es sich an, alle benötigten Daten in einem separaten Archiv zu sichern, das sich in der Verantwortung der Rechtsabteilung befindet. Ist der Rechtsstreit beendet, stößt sie die datenschutzkonforme Löschung an.

Um die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu erfüllen, ist das Unternehmen verpflichtet, die erfolgreiche Löschung nachweisen zu können. Dabei muss es darauf achten, keinen neuen Fundus personenbezogener Daten zu erzeugen. Das Ausführen eines SQL-Löschbefehls und das Speichern der

Ergebnismenge wäre beispielsweise ein neuer Datenbestand, dem allerdings die Rechtsgrundlage fehlt.

Bei einer anlassbezogenen Löschung sind die Verantwortlichen verpflichtet, den gesamten Vorgang der Anfrage zu dokumentieren. Hier kann auch das erfolgreiche Löschen von Daten einfließen. Mit Screenshots, den SQL-Befehlen oder dem negativen Ergebnis einer Suchabfrage ließe sich der technische Vorgang nachweisen.

Schwieriger ist dagegen das Dokumentieren des anlasslosen Löschens nach Zeitablauf. Das erledigen in der Regel automatisierte Skripte, die in den Datenbanken parametrisierte Routinen ausführen. Als Nachweise können hier die Systemeinstellungen gelten, die zeigen, dass die Löschroutinen regelmäßig arbeiten, sowie die Skripte selbst. Zusätzlich müssen die Zuständigen die Parametrisierung der einzelnen Aufrufe und das Ergebnis belegen. Dabei dürfen nur die Informationen im System verbleiben, die die erfolgreiche Ausführung dokumentieren, nicht jedoch die gelöschten Daten selbst.

Backup und Restore sind außen vor

Anders als in Archiven darf in Backups niemand etwas ändern, da deren Zweck in der Wiederherstellung von Daten liegt. Das Herausnehmen einzelner Daten aus einem Backup kann die Konsistenz der Daten verletzen und das Wiederherstellen verhindern. Bei einem Restore geraten jedoch auch die gewollt gelöschten Daten zurück ins System. Um diesen Vorgang datenschutzkonform abzuwickeln, müssen sie im zurückgespielten Datenbestand nochmals gelöscht werden. Das lässt sich beispielsweise anhand der Löschnachweise erledigen. Das Vorgehen beim Wiederherstellen sollte im entsprechenden Verfahren dokumentiert und getestet sein.

Genormtes Vorgehen

Eine gute Grundlage für Löschkonzepte findet sich in der Norm DIN 66398. Sie zeigt eine Vorgehensweise zum Erstellen solcher Konzepte und bietet Orientierungshilfe für Unternehmen aller Größen. Projekte, die das erfolgreich umsetzen wollen, kommen ohne die betroffenen Fachbereiche, die IT-Abteilung und den Datenschutzbeauftragten nicht aus.

Ein solches Projekt könnte nach folgenden Schritten vorgehen (Abbildung 2):

Schritt für Schritt: Vorgehensmodell zum regelkonformen Löschen personenbezogener Daten (Abb. 2)

System-Scoping: Zunächst müssen die Zuständigen alle Systeme ermitteln, die personenbezogene Daten verarbeiten. Hierzu sollte das Unternehmen in einem Regelwerk Datenschutzklassen vorgeben. Häufig erfolgt das Klassifizieren im Rahmen der Schutzbedarfsfeststellung, die neben den Kriterien Vertraulichkeit, Integrität und Verfügbarkeit auch erfasst, ob personenbezogene Daten verarbeitet werden.

Untersuchung der Daten: Weiterhin ist für alle erkannten Systeme detailliert aufzunehmen, um welche Daten es geht. Sie lassen sich dann in vorgegebene Kategorien einsortieren.

Fachliche Löschregeln: Aus den vorliegenden Informationen können die Administratoren nun fachliche Löschregeln ableiten. Dabei ermitteln sie für jede Datenkategorie, ob Aufbewahrungsfristen existieren und welche Löschfristen sich daraus ergeben.

Analyse der Schnittstellen und Abhängigkeiten: Zu den einzelnen Systemen müssen die Fachabteilungen weiterhin die Schnittstellen zu vor- und nachgelagerten Systemen finden und analysieren. Dabei erfassen sie die Quell- und Zielsysteme, die Datenkategorien, die Häufigkeit der Übertragung und die Art der Schnittstelle. Mit dieser Dokumentation können sie Abhängigkeiten untersuchen.

Fachliches Löschkonzept: Aus den gesammelten Informationen wird ein Löschkonzept erstellt.

Entscheidung für eine Löschlösung: Abhängig von der Analyse muss das Unternehmen eine Löschstrategie formulieren – etwa, ob es eine zentrale, eine dezentrale oder eine Mischlösung einführen will.

Technische Löschkonzepte: Sie beschreiben die konkrete Durchführung des Löschens. Auch Produktion und Ablage der Löschnachweise werden hier dokumentiert.

Test: Vor der Einführung der Löschroutinen müssen diese ausführlich geprüft werden. Dabei sind sowohl die vollständige Löschung innerhalb des Systems als auch die Abhängigkeiten zu anderen Systemen einzubeziehen.

Umsetzung: Nach erfolgreichem Test können die Zuständigen die Löschroutinen auf die einzelnen Systeme loslassen. In der Regel kann die Einführung in Stand-alone-Systemen, die keinerlei Schnittstellen nach außen haben, unabhängig vom Rest der IT-Welt erfolgen. Die meisten Systeme sind jedoch mit anderen verbunden und müssen gleichzeitig in Produktion genommen werden.

Ablage der Nachweise: Darüber muss ebenfalls eine Entscheidung fallen. Eine zentrale Löschlösung bietet oftmals eine Ablagemöglichkeit an. Wird dezentral gelöscht, müssen die Zuständigen über eine gemeinsame Ablagemöglichkeit und einen Prozess nachdenken, der die Nachweisführung sicherstellt.

Fazit

Das Ganze ist genauso kompliziert, wie es sich anhört. Die Vielzahl der Systeme, die Abhängigkeiten, der Umfang der Daten und ihre Redundanz erschweren die Umsetzung. Hinzu kommt, dass mit dem Löschen von Daten ein Kulturwandel einhergeht, da der jederzeitige Zugriff auf Daten in Vor-DSGVO-Zeiten wichtiger schien als das datenschutzkonforme Löschen.

Die mit der Einführung der Datenschutz-Grundverordnung drastisch gestiegenen und von den Aufsichtsbehörden inzwischen auch durchgesetzten Bußgelder sollten reichen, den Unternehmen das Umdenken zu erleichtern. Bei entsprechenden Projekten muss man sich auf möglicherweise lange Laufzeiten von mehreren Monaten bis zu einigen Jahren einstellen. (jd@ix.de) Frank Heisel

war bei einer Big-Four-Wirtschaftsprüfungsgesellschaft als verantwortlicher Prüfungsleiter für System-, Prozess- und IKS-Prüfungen tätig. Er ist als externer Datenschutzbeauftragter für mehrere Unternehmen benannt und berät Unternehmen zum Thema Datenschutz und internes Kontrollsystem.

[/expand]

DSGVO – 11/2020 – Löschung personenbezogener Daten

DSGVO – 11/2020 – Löschung personenbezogener Daten

[expand title="mehr lesen…"]

Löschung personenbezogener Daten

Seid sparsam

Tobias Haar

Das Datenschutzrecht verlangt die Löschung personenbezogener Daten, wenn sie nicht mehr rechtmäßig verarbeitet werden dürfen. Wann und wie das zu erfolgen hat, ist oft eine schwierige Einzelfallentscheidung.

-tract

- Das Datenschutzrecht verlangt die Löschung personenbezogener Daten, wenn in Unternehmen oder Organisationen der Verarbeitungszweck dieser Daten entfällt oder keine Einwilligung des Betroffenen vorliegt.
- Schwierigkeiten bei der Erfüllung der Vorgaben bereiten zu wenig spezifizierte Regelungen und Definitionen, einander widersprechende Speicherfristen, eine Datenverarbeitung durch Dritte und mehr.
- Was die DSGVO letztlich fordert, ist ein verantwortlicher, gesetzeskonformer Umgang mit personenbezogenen Daten im Rahmen eines auf die eigene Organisation zugeschnittenen Datenschutz- und -löschkonzepts.

Die Datenschutz-Grundverordnung hat sich mit ihren Pflichten in den letzten zwei Jahren zum Angstgegner vieler Unternehmen entwickelt. Die drohenden Bußgelder sind enorm, das Risiko von Abmahnungen durch Konkurrenten und Verbände ist real. Auf der anderen Seite müssen Unternehmen personenbezogene Daten mitunter ein Jahrzehnt oder noch länger speichern, um ihren vertraglichen und gesetzlichen Pflichten zu genügen. Eine nicht immer einfache Gratwanderung – im Detail entstehen unlösbar erscheinende Konflikte. Hier den Überblick zu behalten, ist selbst für Juristen und Datenschutzbehörden eine stetige Herausforderung, zumal sich die Rahmenbedingungen auch ändern.

Um sich dieser Herausforderung zu stellen, hilft es, die zugrunde liegenden Vorgaben des Datenschutzrechts zu kennen. In Zweifelsfällen muss man sich damit behelfen, herauszufinden, was die jeweilige Intention des Gesetzgebers für bestimmte gesetzliche Regelungen ist. Um Unternehmensentscheider hierbei zu unterstützen, ist die Bestellung eines betrieblichen Datenschutzbeauftragten für viele Unternehmen verpflichtend. Hilft all dies nicht, bleibt stets die Möglichkeit, sich ratsuchend an die Datenschutzbehörden zu wenden. Das ist im Einzelfall womöglich immer noch besser, als sich bei Mängeln in der Compliance erwischen zu lassen. Es gibt erste Bußgeldentscheidungen der Datenschutzaufsicht, die das belegen. Hier zeigen sich Parallelen zum Kartell- und Wettbewerbsrecht, das Kooperation (und mitunter auch das Auftreten als Kronzeuge) belohnt.

Das geschützte Gut

Was schützt das Datenschutzrecht? Es gilt ausschließlich für personenbezogene Daten. Diesen Begriff definiert Art. 4 Nr. 1 DSGVO ausführlich und auch anhand von Beispielen als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person') beziehen; als identifizierbar wird eine natürliche

Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“.

Diese Definition reicht sehr weit. Es gilt – und das wurde bereits vom Europäischen Gerichtshof entschieden – ein objektiver Datenbegriff. Es kommt nicht darauf an, ob ein für die Datenverarbeitung verantwortliches Unternehmen mit vorhandenen Daten einen Bezug zu einer „identifizierte[n] oder identifizierbare[n] natürliche[n] Person“ herstellen kann. Es kommt darauf an, ob es irgendeine Stelle auf der Welt gibt, die etwa aus mehreren Datenpunkten einen Personenbezug herstellen könnte. Oftmals wird eingeschränkt, dass der Bezug eines Datums zu einer Person mit „verhältnismäßigen Mitteln“ herstellbar sein muss.

Als bekanntes Beispiel dienen IP-Adressen. Ein Webseitenbetreiber kann alleine aus der IP-Adresse eines Webseitenbesuchers nicht auf dessen Person Rückschlüsse ziehen. Weil es aber der Internetzugangsprovider kann, liegt auch für den Webseitenbetreiber ein personenbezogenes Datum vor und die Pflichten aus der DSGVO greifen. Hier zeigen sich Schnittstellen zur umstrittenen Vorratsdatenspeicherung. Auch sie führt rechtlich zu einer Pflicht des Internetanbieters, bestimmte Daten nicht zu löschen.

Es gibt in Art. 5 der DSGVO für die Datenverarbeitung übergreifende Grundsätze, die im Umgang mit personenbezogenen Daten stets berücksichtigt werden müssen: Diese müssen rechtmäßig und für den Betroffenen transparent verarbeitet werden. Sie unterliegen einer Zweckbindung und dürfen nicht ohne Weiteres für andere Zwecke verarbeitet werden. Ihre Verarbeitung muss auf das notwendige Maß reduziert werden. Und schließlich müssen sie richtig und „angemessen sicher“

verarbeitet werden.

Zeitlich begrenztes Speichern

Eine Herausforderung stellt für viele verarbeitende Stellen die Vorgabe der „Speicherbegrenzung“ dar. Danach dürfen personenbezogene Daten nur „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“. Wer diese Vorgaben nicht einhält, muss die Daten löschen.

Die DSGVO regelt dabei nicht, welcher in Tagen, Monaten oder Jahren bemessene Zeitraum im Einzelfall gilt. Das „nur so lange“ kann oftmals nur mittels des Zwecks der Datenverarbeitung oder gesetzlicher Vorgaben beantwortet werden. Ist Zweck der Datenverarbeitung die Erfüllung eines Vertrages, zum Beispiel die Lieferung von Versandartikeln, darf der Händler die Daten selbstverständlich für die Bearbeitung der Bestellung, den Versand und die Abrechnung der Lieferung verarbeiten und sie dabei auch speichern.

Im Versandhandel kommt hinzu, dass das Speichern bis zum Ablauf der Widerrufsfrist für Verbraucher gestattet ist. Danach müsste der Händler die Daten jedoch wieder löschen. Spitzfindige könnten bereits argumentieren, dass eine Speicherung bis zum Ablauf der regelmäßigen Verjährungsfrist für Gewährleistungsmängel nicht mehr gestattet ist. Denn im Gewährleistungsfall müsste der Kunde nachweisen, wann und von wem er ein Produkt erworben hat.

Spezialgesetz sticht Datenschutz

An dieser Stelle „hilft“ das Steuer- und das Handelsrecht. Danach müssen etwa Rechnungen bis zu zehn Jahre aufbewahrt werden. Diese Vorschriften haben als Spezialgesetz Vorrang vor dem Datenschutzrecht. Erst nach zehn Jahren dürfen die Rechnungen gelöscht werden, nach Datenschutzrecht müssen sie

das dann aber auch. Auch Buchungsbelege, „Bücher und Aufzeichnungen“ und andere Unterlagen unterliegen dieser Aufbewahrungsfrist.

Nur sechs Jahre aufzubewahren sind empfangene und abgesandte Handels- und Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind. Auch E-Mails mit entsprechendem Inhalt können „Briefe“ nach diesen Vorgaben sein. Anstatt zu löschen, müssen Unternehmen insbesondere bei ausscheidenden Mitarbeitern prüfen, ob sie deren E-Mail-Accounts weiterhin verfügbar halten müssen, um bei Bedarf darauf zugreifen zu können.

Bei Verträgen kommt meist hinzu, dass die Aufbewahrungsfrist erst mit Ende der Vertragslaufzeit zu laufen beginnt. Enthalten sie etwa personenbezogene Daten eines Vermieters, müssen sie trotz der Vorgaben des Datenschutzrechts sechs volle Jahre nach Ende des Mietvertrags aufbewahrt werden. Die Fristen können sich beispielsweise bei laufenden Steuerverfahren zudem verlängern. Eine Verletzung der Aufbewahrungspflicht kann mit Bußgeldern belegt werden oder zu unangenehmen Steuerschätzungen führen. Können Beweise in Gerichtsverfahren wegen Löschung nicht mehr vorgelegt werden, drohen finanzielle Nachteile durch entsprechende Urteile.

Die Art und Weise der Aufbewahrung von Steuerunterlagen ergibt sich aus den „Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“ [1]. Auch IP-Adressen mit Zeitstempel können steuerrelevante Informationen sein, die aufbewahrt werden müssen. Sie können beispielsweise gebraucht werden für den Umsatzsteuernachweis, ob eine „elektronisch erbrachte Dienstleistung“ von einem Verbraucher in Deutschland (16% bzw. 19% Umsatzsteuer) oder etwa in Ungarn (dann 27%) abgerufen wurde. Hierzu zählen etwa Streaming, Premium-Features in Computerspielen, E-Books, Software- oder App-Downloads und dergleichen.

Die Behörde – dein Freund und Helfer

Den meisten Steuerbehörden genügt es, wenn eine IPv4-Adresse um das letzte Oktett verkürzt gespeichert wird, um diesen Nachweis zu führen. Ähnliches gilt für teilgeschwärzte Kreditkartennummern oder eine IBAN. Im Einzelfall ist hier eine Abstimmung sowohl mit den Steuerbehörden als auch mit den Datenschutzbehörden erforderlich. Als Unternehmen kann man auch beide Behörden bitten, die Diskussion gemeinsam zu führen und eine gemeinsame Lösung zu erarbeiten.

Der Grundsatz der Datensparsamkeit und Zweckbindung verlangt, die personenbezogenen Datensätze nach Zweckerreichung aus allen Systemen zu löschen, die nicht für steuerliche Belange eingesetzt werden. Hierzu zählt etwa ein Customer-Relationship-Management-System (CRM). Die Pflicht zur Speicherung von Daten umfasst aber nicht auch das Recht, diese in sämtlichen Systemen stets verfügbar zu halten. Die Zweckbindung verlangt, dass nur insoweit gespeichert wird, wie die Daten auch künftig benötigt werden. Eine Ausnahme ist dann möglich, wenn ein Betroffener einer längeren Datenspeicherung zugestimmt hat. Dies kommt beispielsweise bei Kundenaccounts von Amazon und Co. in Betracht. Ob diese Einwilligung stets nach DSGVO-Grundsätzen wirksam ist, ist eine andere Frage.

Auch aus anderen Rechtsbereichen ergibt sich eine Pflicht zur Aufbewahrung personenbezogener Daten. Das gilt etwa für das Arbeitsrecht, das Sozialversicherungsrecht, das Produkthaftungsgesetz et cetera. Die IHK Pfalz stellt eine Übersicht zur Verfügung (siehe ix.de/zy59), die auch kurios anmutende Kategorien wie „Essensmarkenabrechnungen“ auflistet.

Nicht mehr dem Zweck entsprechend benötigte und keinen Aufbewahrungspflichten mehr unterliegende personenbezogene Daten sind zu löschen. Das ergibt sich bereits aus allgemeinen Datenschutzgrundsätzen, insbesondere aber aus Art. 17 der DSGVO. Diese Vorschrift regelt das „Recht auf Vergessenwerden“. Sie spiegelt die Pflichten nach Art. 5 der

DSGVO und verlangt vor allem die Löschung bei Zweckwegfall, Widerruf einer Einwilligung und unrechtmäßiger Verarbeitung. Es handelt sich dabei um ein Recht des Betroffenen gegenüber der Daten verarbeitenden Stelle. Das bedeutet aber nicht, dass eine Löschung nur dann stattfinden muss, wenn er dieses Recht explizit geltend macht. Wann immer keine gesetzliche Rechtfertigung oder wirksame Einwilligung des Betroffenen vorliegt, müssen personenbezogene Daten gelöscht werden.

Die DSGVO definiert nicht, was rechtlich unter Löschung zu verstehen ist. Das war bis zum Inkrafttreten der früheren Fassung des Bundesdatenschutzgesetzes noch anders, dort war das Löschen von Daten als das „Unkenntlichmachen von Daten“ festgelegt. So definieren es auch Wikipedia und Gerichtsurteile nach dem Strafgesetzbuch, etwa beim strafbaren „Ausspähen von Daten“.

Den Personenbezug entfernen

Löschung personenbezogener Daten bedeutet allerdings nicht, dass die Daten auch physisch vernichtet werden müssen. Es genügt, wenn ihnen der Personenbezug genommen wird. Das ist ein bedeutender Unterschied, wie die österreichische Datenschutzbehörde auf Anfrage eines Versicherungsunternehmens geklärt hat. Werden personenbezogene Daten zu anonymisierten Daten, dürfen sie nach der DSGVO auch weiterhin zeitlich unbefristet verarbeitet werden. Die DSGVO ist auf solche Daten schlicht nicht anwendbar.

Einen Grenzfall bildet die Pseudonymisierung personenbezogener Daten. Im Erwägungsgrund 26 zur DSGVO heißt es dazu: „Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.“ Fachleute deuten das Wort „sollten“ als Einschränkung dahingehend, dass es datenschutzrechtlich vertretbar ist, wenn die Verbindung zwischen einem

pseudonymisierten Datum und einer Person nur mit erheblichem Aufwand für die verarbeitende Stelle oder einen Dritten herzustellen ist. Was unter einem „erheblichen Aufwand“ zu verstehen ist, muss im Einzelfall entschieden werden.

Um sich der technischen Herausforderung der Löschung von Daten oder jedenfalls des Personenbezugs zu nähern, bieten Abschnitt CON. 6 „Löschen und Vernichten“ im IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik oder etwa DIN 66399 praktische Anleitungen (siehe ix.de/zy59). Der Schwerpunkt liegt dabei aber auf der Vernichtung im Sinne von sicherer Entsorgung von Datenträgern et cetera, die dann als datenschutzkonform gelöscht gelten.

Unternehmen müssen diesen Vorgaben und weiteren Abschnitten im IT-Grundschutz zufolge bei Bedarf ein Datenlöschkonzept erarbeiten und umsetzen, das auf die individuellen Gegebenheiten ausgerichtet ist. Dies fordert letztlich auch die DSGVO. Dabei folgt sie dem Ansatz, dass Daten verarbeitende Unternehmen Datenschutz eigenverantwortlich sowie gemäß den gesetzlichen Vorgaben umsetzen und dokumentieren müssen.

Hilfreich bei der Bestimmung der Löschfristen verschiedener Datenarten und beim Erstellen eines Löschkonzepts kann auch die DIN 66398 sein. Sie ist keine Norm, sondern eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ (siehe Abbildung).

Die Leitlinie DIN 66398 enthält Hilfestellungen für die kniffligen Fragen, die sich Unternehmen im Zusammenhang mit DSGVO-konformem Datenlöschen stellen. *Deutsches Institut für Normung*

Dauerproblem Cloud

Schwierig wird die Datenlöschung oft dann, wenn externe Anbieter im Auftrag Daten verarbeiten oder speichern. Hierzu zählen auch Cloud-Anwendungen. Bei deren Auswahl muss ein

Unternehmen darauf achten, dass die DSGVO-Vorgaben eingehalten werden und eben auch das Löschen personenbezogener Daten sicher und nachhaltig möglich ist. Das Datenschutzrecht unterscheidet bei der Verantwortlichkeit nicht, ob ein Unternehmer selbst oder ein (Cloud-)Dienstleister für ihn personenbezogene Daten verarbeitet.

Recherchen nach Anbietern im Bereich Datenvernichtung und Datenlöschung über Suchmaschinen führen zu einer großen Anzahl an Treffern. Die Auswahl eines solchen Anbieters ist schwierig. Sie muss aber sorgfältig getroffen werden, denn der Verantwortliche kann sich nicht durch Schlamperei oder Fehler eines externen Dienstleisters freizeichnen. Zudem muss ein Auftragsverarbeitungsvertrag nach den Vorgaben der DSGVO abgeschlossen werden, denn der Dienstleister kommt mit personenbezogenen Daten in Berührung. Befindet sich die Cloud außerhalb der EU – etwa in den USA – oder lässt sich dies nicht ausschließen, tauchen weitere datenschutzrechtliche Hürden auf. Jüngst wurde dies durch die EuGH-Entscheidung „Schrems II“ zur Unwirksamkeit des EU-US Privacy Shield deutlich (siehe *iX* 9/2020).

Das Datenschutzrecht ist grundsätzlich selbst bei unverhältnismäßig großem Aufwand für die Einhaltung der Vorgaben zu befolgen. In gewissem Umfang hilft Unternehmen hier, dass auch nach der Einführung der DSGVO anhand objektiver Kriterien geprüft werden kann, ob die Umsetzung von Löschpflichten im Einzelfall verhältnismäßig ist. Ist sie das nicht, besteht unter Umständen die Möglichkeit, personenbezogene Daten zu sperren, statt sie zu löschen.

Die DSGVO spricht hier auch von einer „Einschränkung der Verarbeitung“. Sie erfordert entsprechende technische und organisatorische Maßnahmen. Beispielsweise kann der Datenzugang innerhalb eines Unternehmens mittels Passwort auf wenige Personen beschränkt werden oder die Daten werden in andere Datenbanken übertragen, die gleichfalls nur beschränkt zugänglich sind. Wie stets müssen Lösungen erarbeitet werden,

die den jeweiligen Einzelfall DSGVO-konform abbilden.

Zur Reduzierung des Aufwands kann eventuell auch ein Data Lifecycle Management beitragen, also eine richtlinienbasierte Lösung, die bei Erreichen bestimmter Parameter zu einer automatischen Löschung von Daten führt. Dabei dürfen jedoch keine Fehler bei der Definition der Parameter auftreten – sie könnten zu hohen Folgeschäden führen.

Im Zweifel muss nach DSGVO eine personenbezogene Datenverarbeitung unterbleiben, wenn die Verarbeitung unzulässig oder auch die sichere Löschung unmöglich erscheint. So die Theorie. In der Praxis helfen Orientierungshilfen und andere Veröffentlichungen von Datenschutzbehörden in vielen Fällen dabei, die Vorgaben des Datenschutzrechts einzuhalten. Und oftmals müssen Unternehmer auch die Entscheidung treffen, ein verbleibendes Risiko einzugehen. Bis Einzelfragen gerichtlich geklärt sind, vergehen oft etliche Jahre. In Einzelfällen ist auch ein Spiel auf Zeit denkbar, wenn die Chancen die Risiken überwiegen. Angesichts der signifikant erhöhten Bußgelder kippt dieses Verhältnis aber zunehmend in Richtung eines inakzeptablen Risikos. Das ist vom Gesetzgeber auch durchaus gewollt.

Fazit

Die Frage, wie lange personenbezogene Daten gespeichert werden dürfen oder sogar müssen, muss jedes Unternehmen für sich entscheiden: Zahlreiche Spezialgesetze verlangen eine Speicherung auch über den eigentlichen Zweck hinaus. Hierbei hilft nur ein Ansatz über alle Unternehmensbereiche hinweg, der in ein Datenschutzkonzept mündet. Wann und wie personenbezogene Daten zu löschen oder zu vernichten sind, muss ebenfalls enthalten sein.

Dieses Thema ist für Unternehmen aber nur ein Ausschnitt aus der Gemengelage, wie sie mit Daten allgemein umzugehen haben. Neben personenbezogenen Daten muss auch für andere

„geschäftliche Informationen“ Ort, Dauer und Zweck einer Speicherung festgelegt werden. Auch hier gilt es, deren Löschung zu regeln. Das Gesetz zum Schutz von Geschäftsgeheimnissen verlangt die Erstellung eines Geheimnisschutzkonzepts. Es hilft alles nicht, Unternehmen müssen ihren Umgang mit Daten ganzheitlich angehen, um ihre eigenen Interessen zu vertreten und gesetzlichen Vorgaben zu entsprechen. Dienstleister können hier zwar helfen, die Verantwortung bleibt aber beim Unternehmen, um dessen Daten es geht. (ur@ix.de)

1. Quellen
2. Tobias Haar; Digitalbeleg; Neue Vorgaben zur elektronischen Buchführung; *iX* 3/2020, S. 92
3. Tobias Haar; Weckruf; EU-US Privacy Shield scheitert vor EuGH; *iX* 9/2020, S. 44
4. Die für das Datenlöschen relevanten DIN-Normen und das entsprechende BSI IT-Grundschutzkapitel sowie die IHK-Liste der verschiedenen Datenkategorien sind über ix.de/zy59 zu finden.

Tobias Haar, Rechtsanwalt, LL.M. (Rechtsinformatik), MBA,

ist Rechtsanwalt mit Schwerpunkt IT-Recht bei Vogel & Partner in Karlsruhe.

[/expand]

DSGVO – 11/2020

DSGVO – 11/2020

[expand title="mehr lesen…"]

Wo versteckte personenbezogene Daten lauern

Böse Überraschung

Martin Gerhard Loschwitz

Durch die Löschpflicht der DSGVO können vergessene Datensenken im Unternehmen zu einem echten Problem und verdammt teuer werden. Wo liegen heikle Daten, wie stöbert man sie auf und wie verhält es sich mit WORM-Archiven? iX hilft bei der Spurensuche.

-tract

- Die DSGVO sieht Löschpflichten für personenbezogene Daten vor, die nicht länger benötigt werden.
- Für Administratoren gerät der Versuch, die DSGVO-Vorschriften unter anderem mit Archivierungspflichten in Einklang zu bringen, oft zu einer Gratwanderung.
- Vielen Unternehmen ist gar nicht klar, wo sie überhaupt personenbezogene Daten speichern.
- Wichtig ist es, IT-Verantwortliche für versteckte Datensenken mit personenbezogenen Daten zu sensibilisieren, denn die technischen Lösungen für das Problem sind komplex und in vielen Fällen unbefriedigend.

Man stelle sich im eigenen Unternehmen die folgende Situation vor: Der Drucker druckt nicht. Alles Wackeln am Kabel vermag

das Problem nicht zu beseitigen, und letztlich stellt sich heraus, dass der Kollege Niemeyer sich auf seinem Rechner einen Virus eingefangen hat, der das gesamte System lahmlegt. Weil Herr Niemeyer sich den Virus eingefangen hat, indem er auf dubiosen Seiten unterwegs war, und weil seine Personalakte weitere unschöne Einträge enthält, setzt das Unternehmen ihn vor die Tür.

Ein halbes Jahr später – der Prozess vor dem Arbeitsgericht gegen Herrn Niemeyer ist noch in vollem Gange – flattert ein Brief der Landesdatenschutzbehörde ins Haus. Der Rechtsabteilung zieht es prompt die Schuhe aus: 500000 Euro, so heißt es dort, werden in Form einer Strafe wegen Verstoßes gegen die DSGVO fällig. Die Behörde habe stichhaltige Beweise dafür, dass das Unternehmen es seit Jahren versäume, Daten mit persönlichem Bezug im Sinne der DSGVO zu löschen, wenn diese nicht länger benötigt würden.

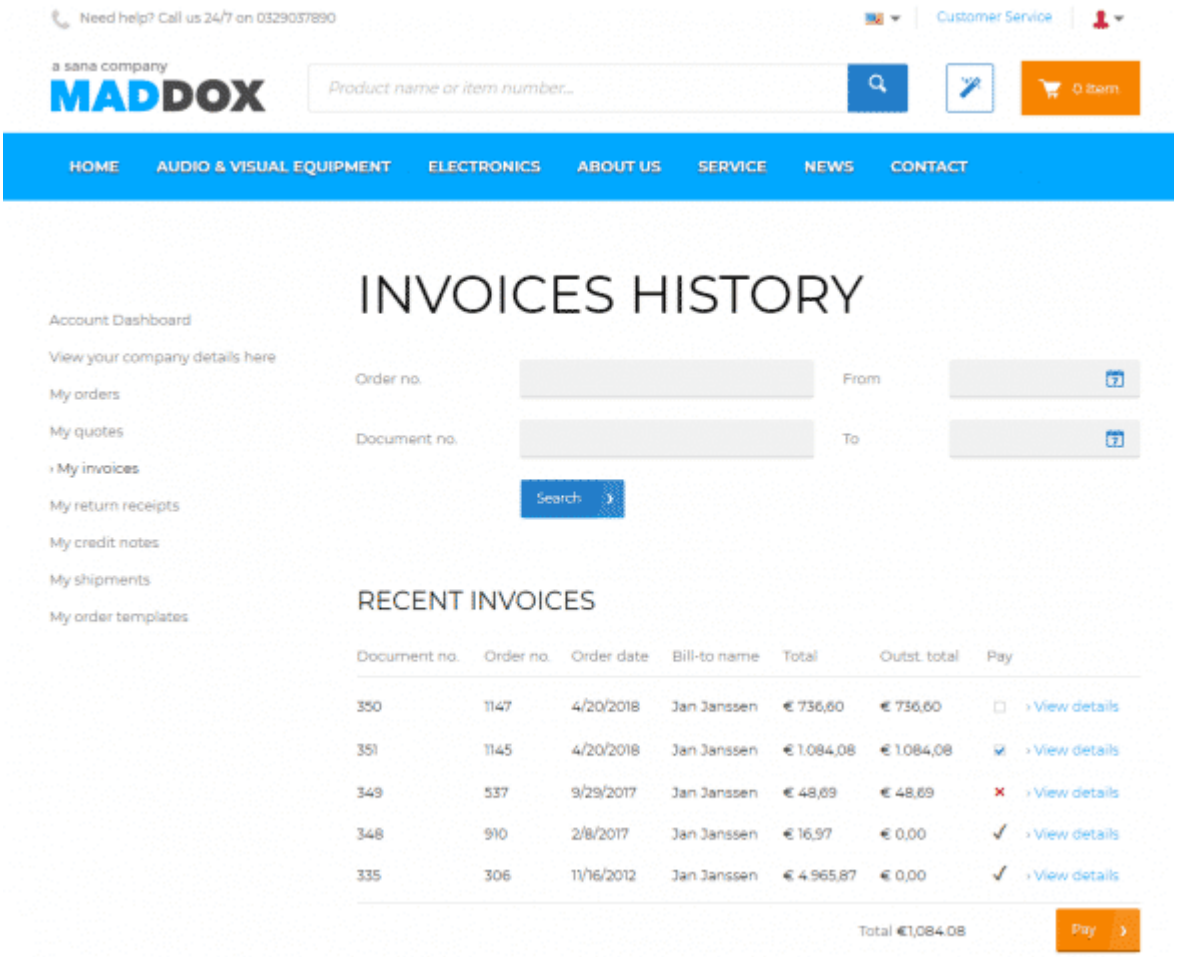
Klingt wie das Drehbuch eines schlechten Films, ist leider aber überhaupt nicht unwahrscheinlich. Die Datenschutzbehörden der Länder gehen mittlerweile alles andere als zimperlich mit Verstößen im DSGVO-Kontext um, wie das Beispiel Deutsche Wohnen eindrücklich bestätigt. Maja Smoltczyck, die Landesdatenschutzbeauftragte von Berlin, will von der Wohnungsgesellschaft 14,5 Millionen Euro Bußgeld eintreiben, und das mit eben diesem Vorwurf. Zwar wehrt sich die Deutsche Wohnen mit Händen und Füßen und wohl bald auch vor Gericht gegen den Bußgeldbescheid. Und in diesem Fall liegen die Dinge auch etwas anders, weil es hier nicht ein ehemaliger Mitarbeiter war, der den Stein ins Rollen brachte, sondern eine Kooperation mehrerer Datenschutzgruppen.

Das Beispiel zeigt jedoch eindrücklich: Die in der DSGVO festgeschriebene Löschpflicht kann für Unternehmen im Fiasko enden, ohne dass diese auch nur den leisesten Verdacht hätten, was da auf sie zurollt. Und Mitarbeiter mit Rachegelüsten, die über unzulässige Datensenken im Sinne der DSGVO im Unternehmen Bescheid wissen, können erheblichen Schaden anrichten.

Welche Optionen sich Firmen bieten

Was aber können Unternehmen tun? Eines sei gleich am Anfang dieses Artikels gesagt – das Ziel besteht an dieser Stelle nicht darin, über die Löschpflicht im Sinne der DSGVO zu debattieren oder im Detail auf sie einzugehen. Wer sich für die juristischen Spitzfindigkeiten interessiert, möge sich die anderen Artikel der Titelstrecke in dieser Ausgabe zu Gemüte führen. Hier geht es vielmehr um die Praxis – um die IT-Abteilung, die sich als Dienstleister für digitale Services im Unternehmen versteht und mit der DSGVO irgendwie umgehen muss. In dieser Position haben Systemverwalter das ausgesprochen unangenehme Problem, zwischen mehreren Stühlen zu sitzen. Denn bei ihrer alltäglichen Arbeit sind sie ja nicht nur den Regeln der DSGVO unterworfen, sondern auch anderer relevanter Gesetzgebung. Das Finanzamt etwa schreibt vor, dass bestimmte Arten von Belegen revisionssicher über Jahre und Jahrzehnte hinweg für spätere Überprüfungen aufzubewahren sind. Damit besteht im Sinne der DSGVO eine „andere Rechtsgrundlage“ für das Speichern von Daten.

Der Teufel steckt allerdings im Detail: Viele Softwarepakete etwa bieten erst gar keine Möglichkeit, nur bestimmte Teile eines Datensatzes zu löschen, andere jedoch zu erhalten. Verlangt ein Kunde etwa die Löschung seines Benutzerzugangs in einem Webshop, muss das Unternehmen dem Ansinnen grundsätzlich nachkommen, darf aber natürlich die Unterlagen behalten, die aufzubewahren es verpflichtet ist. Die meisten Webshops bieten dafür aber keine Funktion: Wer den Zugang löscht, löscht meist auch sämtliche damit verbundenen Dokumente.



Die DSGVO stellt Unternehmen vor allem bei komplexen Anwendungen wie Shopsystemen vor das Problem, Archivierungs- und Löschpflichten unter einen Hut zu bekommen (Abb. 1). *SANA Commerce*

Ähnliches gilt für Daten, die das Unternehmen nach dem WORM-Prinzip (Write Once, Read Many) zu archivieren verpflichtet ist. Hier kommen oft Hardware-Appliances zum Zug, die den gesetzlichen Vorgaben genügen. Vielfach haben sich Firmen bisher mit dem Thema DSGVO aber nicht ausführlich genug beschäftigt und archivieren ihre Daten erst gar nicht ausreichend fein abgestuft, um der DSGVO zu genügen.

Primär soll dieser Artikel Administratoren sensibilisieren und ihnen Anhaltspunkte dafür liefern, wo sich auf klassischen Serversystemen bedenkliche Daten befinden können. Der Text geht auch auf die Frage ein, welchen Aufwand im Sinne des DSGVO-konformen Speicherns von Daten sie betreiben sollen und müssen und wie sich das mit Tools angenehmer gestalten lässt. Vorrangig jedoch geht es darum, wie Administratoren ihre Sinne

schärfen, um potenziell gefährliche Datensenken im Unternehmen zu erkennen und zu eliminieren.

Datensenken

Der Begriff Datensenke stammt ursprünglich aus den Definitionen im Umfeld von Datenübertragungseinrichtungen (siehe ix.de/z9h2). Dort bezeichnet er eine empfangende Datenendeinrichtung.

In der IT gilt ein weiter gefasster Begriff: Einerseits zählt man nicht nur „empfangende“ Dienste wie Mailserver dazu, sondern generell alle Geräte und Dienste, die Daten vorhalten oder ablegen, vom Benutzerverzeichnis über Datenbanken, Geschäftsanwendungen, Shopsysteme bis hin zu smarten Endgeräten, Syslog-Diensten und Systemeinstellungen. In der Praxis bezeichnet man vor allem solche Orte als Datensenken, wo Daten hingesendet werden, um dort zu versacken – also genau das, was im DSGVO-Kontext zu vermeiden ist.

Viele Unternehmen haben zu wenig getan

Viele Unternehmen müssen sich den Vorwurf gefallen lassen, sich mit dem Thema der in der DSGVO verankerten Löschpflicht erst viel zu spät zu beschäftigen. Als die DSGVO in Kraft trat, gab es die heute aus Sicht von Administratoren unangenehmen Paragrafen ja bereits. Ganze vier Jahre hatten Firmen Zeit, sich technisch auf das vorzubereiten, was eine rigoros angewandte DSGVO für sie bedeuten würde. Passiert ist in dieser Richtung vielerorts wenig.

So ist vielen Verantwortlichen heute leider noch immer völlig unklar, wo in ihren Set-ups personenbezogene Daten anfallen. Viele Admins denken bei personenbezogenen Daten im Sinne der DSGVO zudem automatisch an die Daten der Endanwender. Das ist aber eine unvollständige Sicht auf die Dinge: Der bereits erwähnte Herr Niemeyer hat, wenn im Unternehmen gängige Compliance-Regeln zur Anwendung gekommen sind, einen eigenen

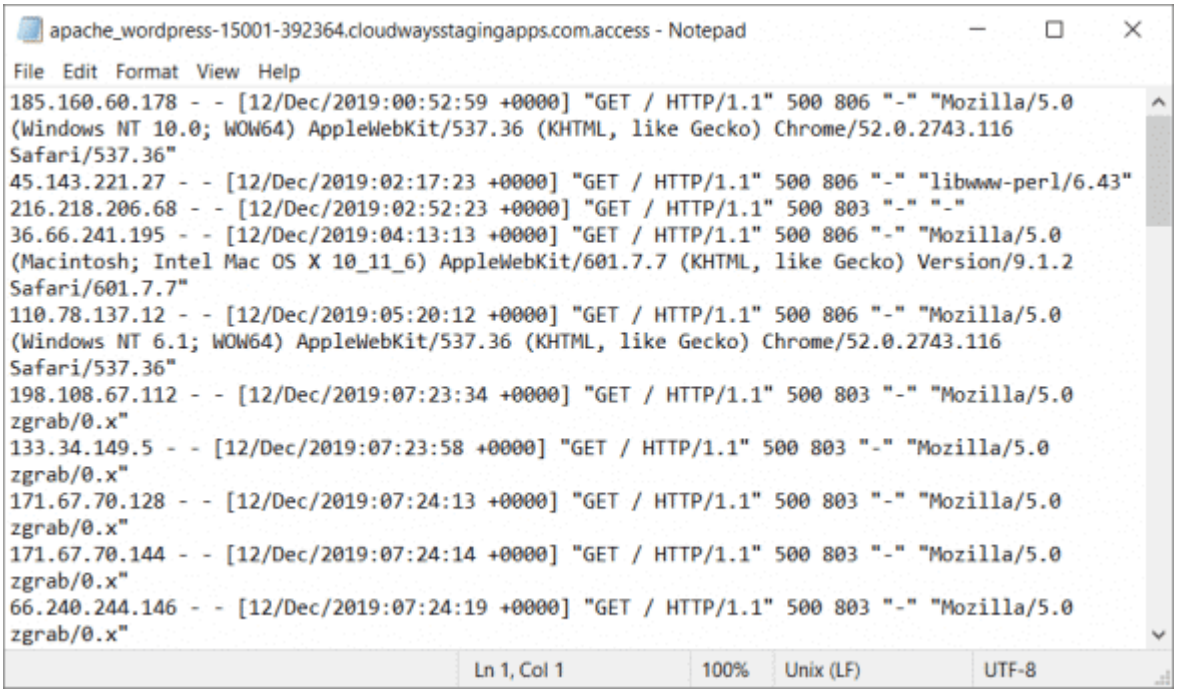
Account gehabt, mit dem er auf den Systemen hantierte.

Personenbezogene Daten sind daher beispielsweise auch die History der Shell, die der nun ehemalige Kollege im Rahmen seiner dienstlichen Tätigkeit genutzt hat. Verlangt er nach einer Einigung vor dem Arbeitsgericht, dass diese Daten entfernt werden, muss die Firma das ebenso tun, wie sie zum Löschen von Kundendaten verpflichtet wäre – freilich unter der einen zentralen Einschränkung, dass jene Daten behalten werden dürfen, zu deren Sicherung die Firma aus anderen Gründen verpflichtet ist.

Dreierlei Werkzeuge im Fokus

Wer vor der Aufgabe steht, Datensenken im eigenen Unternehmen zu finden und zu beseitigen, sieht sich eingangs einer Sisyphusarbeit gegenüber. Denn wenn Hunderte Systeme seit Jahren in Betrieb sind, ist die Wahrscheinlichkeit, dass sich auf diesen personenbezogene Daten finden, ausgesprochen hoch. Grob formuliert gibt es drei Arten von Werkzeugen, mit denen der Admin in diesem Kontext in Berührung kommt.

Da gibt es einerseits die Werkzeuge, die personenbezogene Daten produzieren (etwa die bereits erwähnte Shell in Form ihrer History) oder aufzeichnen (hierzu gehören auch Logdateien aller Art). Dann gibt es die Werkzeuge, deren Aufgabe ja gerade darin besteht, Daten langfristig zu archivieren. Ein solches Werkzeug ist der Firma Deutsche Wohnen zum Verhängnis geworden. Denn die hat Daten wie Gehaltsnachweise, SCHUFA-Auskünfte und ähnliche Unterlagen in ihrem zentralen Archivierungssystem gehabt, lange nachdem die dazugehörenden Mietverträge ausgelaufen waren – ein klarer Verstoß gegen die Löschpflicht, wie Berlins oberste Datenschützerin feststellte.



Ausufernde Webserver-Logs sind keine gute Idee, da auch IP-Adressen zu den personenbezogenen Daten gehören und daher einer Löschpflicht unterliegen (Abb. 2). *Cloudways*

Einfach verzichten können Unternehmen auf diese Geräte aber nicht, denn zum Speichern bestimmter Unterlagen über lange Zeiträume – und zwar revisionssicher – sind sie verpflichtet. Einfache Storage-Systeme reichen hier nicht aus, weil bei bestimmten Datenarten eine nachvollziehbare, nachträglich nicht mehr veränderbare Versionsgeschichte abrufbar sein muss. Dazu kommt spezielle Soft- wie Hardware zum Einsatz, die auf das fein granulierte Speichern von Daten aber nicht ausgelegt ist.

Die dritte Art von Werkzeug sind die Tools, die bei der Suche nach eventuell rechtswidrigen Datensenken unterstützen oder deren Entstehen von vornherein verhindern. Dabei handelt es sich einerseits um klassische Forensikwerkzeuge, mit denen sich versteckte Daten auffinden lassen – andererseits fallen in diese Kategorie aber auch ganz typische Werkzeuge im Kontext der Systemautomation. Die lassen sich möglicherweise auf bestehende Set-ups nur noch schwerlich anwenden, führen vor dem Hintergrund moderner Grundlagen der typischen Systemadministration jedoch dazu, dass Admins das Problem zukünftig umgehen.

Produzenten personenbezogener Daten erkennen

Die erste und oberste Frage bei der Untersuchung einer Umgebung im Hinblick auf personenbezogene Daten ist stets die nach den Datenproduzenten. Welche Programme legen – vor allem unbemerkt – personenbezogene Daten an und speichern sie an Orten, an denen man nicht damit rechnet? Im IT-Kontext der Gegenwart ergeben sich hier leider nahezu beliebig viele Möglichkeiten für Orte, an denen solche Daten anfallen.

Schon ein normales Linux-System bietet eine Vielzahl an Einfallstoren. Stellt man sich etwa einen Host mit Webserver vor, bestehen für die Administratoren vermutlich lokale Benutzeraccounts, über die die Administration erfolgt. Diese beinhalten aller Wahrscheinlichkeit nach zum größten Teil personenbezogene Daten. Teil des Offboardings von Kollegen muss es deshalb sein, auf sämtlichen Systemen etwaige Dateien zu löschen oder rechtskonform zu archivieren, auf die diese Kolleginnen und Kollegen Zugriff hatten. Doch ist es damit noch lange nicht getan, denn personenbezogene Daten fallen auch an anderen Stellen an.

Wer etwa HA-Proxy oder nginx als Load Balancer nutzt, lässt diese vermutlich Logdateien über die Zugriffe anlegen. Ähnliches gilt für Webserver, in deren Logdateien ebenfalls IP-Adressen landen. Der Europäische Gerichtshof hat IP-Adressen – und zwar sowohl dynamische als auch statische – mittlerweile als personenbezogene Daten eingestuft. Damit genießen sie eine besondere Schutzwürdigkeit. Was im Umkehrschluss auch bedeutet: Betreiber von Onlineangeboten dürfen diese Information grundsätzlich nur speichern, wenn damit ein „berechtigtes Interesse“ einhergeht. Die Sicherstellung der Servicequalität sowie die Möglichkeit, im Fehlerfalle Debugging zu betreiben, dürfen wohl als berechtigt wahrgenommen werden.

Wer auf seinen Webservern jedoch Logdateien der vergangenen sechs Monate hat, wird sich mit dem berechtigten Interesse schon schwerer tun: Warum etwa sollte es für den Betrieb eines Webshops von Relevanz sein, ob Ottilie Normalverbraucherin vor drei Monaten eine Bestellung aufgegeben hat, die zwischenzeitlich längst geliefert wurde und somit erledigt ist? Wer nicht schon aus Platzgründen Logrotation betreibt, tut auch im Sinne der DSGVO gut daran, diese zu aktivieren. Analoge Empfehlungen gelten auch für andere Geräte im Netzwerk, etwa Firewalls oder Systeme, die zur Intrusion Detection zum Einsatz kommen.

Datenbanken und Backups: Schatzkiste für Datenschützer

Nahezu jedes zeitgenössische IT-Set-up wird irgendwo eine Datenbank enthalten. Das ist völlig legitim, wenn die gespeicherten Daten nötig sind, um die Geschäftsbeziehung und die beiderseitigen Pflichten zu erfüllen. Das eingangs schon erwähnte Problem der Belege ist mittlerweile vielerorts dringend. Hier treffen zwei Rechtsmaterien aufeinander: die Pflicht der Shopbetreiber, Unterlagen für das Finanzamt aufzubewahren, und die Pflicht, benutzerbezogene Daten zu löschen, wenn sie diese nicht länger benötigen.

Aber: Auf die Datenbank selbst haben Systemverwalter in aller Regel keinen direkten Zugriff. Dieser geschieht oft durch eine Software hindurch, etwa eine Shopsoftware, die die Datenbank im Hintergrund nach eigenem Gutdünken verwaltet. Zwar könnte der Admin händisch an der Datenbank herumpulen – garantieren, dass der Shop danach noch funktioniert, wird dann aber keiner. Die Shopsoftware hingegen bietet die Funktion „Account löschen, aber Belege behalten“ oft einfach nicht. Zwar darf der Admin sich an dieser Stelle mit Fug und Recht aufregen, schließlich hatten die Shopbetreiber seit 2013 Zeit, entsprechende Funktionen einzubauen. Das nicht getan zu haben, grenzt hart an Vorsatz. Doch hat der Admin davon nichts, wenn

ihm die Datenschützer an den Fersen kleben.

Eine befriedigende Lösung gibt es an dieser Stelle leider nicht. Es empfiehlt sich, mit dem Betreiber von Software in Kontakt zu treten und sich über deren abgelegte Daten im Detail zu informieren. Die DSGVO sieht in engen Grenzen Ausnahmen für die Fälle vor, in denen das Löschen dem Anbieter nicht zumutbar ist – dazu später mehr. Möglicherweise lässt sich an der jeweiligen Stelle eine solche Ausnahme zur Anwendung bringen.

Vorsicht ist auch bei Backups geboten. Datenbanken und jede Art von Nutzdaten landen heute zuverlässig in Backups. Systeme mit niedrigem Automatisierungslevel legen zudem oft Logs und andere Nutzdaten in Backups ab. Für diese gilt dasselbe wie für die Daten auf den ursprünglichen Systemen auch: Wer etwa seine Datenbank zwar regelmäßig um nicht länger benötigte Daten erleichtert, diese aber weiterhin im Backup hat, gewinnt in Sachen Datenschutz gar nichts. Theoretisch müssten Backups regelmäßig ebenfalls auf entsprechende Daten untersucht werden, um diese zu löschen. Hier wird der Admin im Normalfall aber nicht mehr ohne juristische Hilfe auskommen, schon um zu erfassen, welche Daten zu löschen sind und welche erhalten bleiben dürfen.

Aufgepasst bei Managementtools

Auch bei Software, die im Büro organisatorischen Zwecken dient, ist erhöhte Vorsicht geboten. Nutzt die Assistenz der Geschäftsführung etwa spezielle Werkzeuge, um Termine der Chefs zu managen – beispielsweise Buchungssoftware für Restaurants –, werden diese schnell eine wahre Goldgrube im Hinblick auf personenbezogene Daten sein. Gerade das ist aber ein hervorragendes Beispiel für Daten mit sehr geringer Halbwertszeit.

Ob man mit der Repräsentantin eines anderen Unternehmens vor zwei Monaten im Café Einstein um 15 Uhr einen Kaffee getrunken

hat oder nicht, mag eine Information sein, die zu speichern legitim ist – etwa aus Gründen der Unternehmensstrategie. In der Mehrzahl der Fälle dürfte ein schneller Kaffee aber nicht von so großem strategischen Interesse sein, dass es legitim wäre, Aufenthaltsorte und -zeiten mehrerer Personen dauerhaft zu speichern. Blöd, wenn solche Daten dann über Jahre und Jahrzehnte erhalten bleiben, weil die Datenbank des Terminverwaltungstools nicht regelmäßig um alte Einträge erleichtert wird. Fällt ein solches Werkzeug bei einer DSGVO-Kontrolle den Prüfern auf, händigt man der Behörde am besten gleich die Zugangsdaten zum Onlinebanking für das Firmenkonto aus, das spart Zeit und Mühe.

Alles noch viel schlimmer: Hardware

Eine Misere, die Administratoren fast gar nicht auf dem Schirm haben, sind Clients und spezielle Geräte für die direkte Nutzung durch Anwender. Wer es etwa extrem praktisch findet, dass sich der Nobel-Kaffeevollautomat im Büro per App steuern lässt und für unterschiedliche Nutzer Geschmacksprofile für den Wunschkaffee anlegen kann, denkt besser noch mal nach. Denn ein Kaffeeprofil, das sich auf dem Gerät einer bestimmten ID oder einer MAC-Adresse zuweisen lässt, ist eindeutig zur jeweiligen Mitarbeiterin oder zum jeweiligen Mitarbeiter zurückverfolgbar. So praktisch das Feature also auch sein mag: Datenschutzrechtlich fährt ein Unternehmen besser, wenn es einen Bogen um derartige Funktionen macht. Denn ganz ehrlich: Wer denkt schon daran, beim Offboarding von Kolleginnen und Kollegen die Kaffeemaschine im Büro auf personenbezogene Daten hin zu untersuchen?

Das Internet of Things klingt verheißungsvoll und bringt Endanwendern nützliche Features, die für Firmen vor dem DSGVO-Hintergrund oft heikel sind (Abb. 3). *Melitta*
Ebenfalls beliebt in diesem Kontext sind Geräte, auf denen einmalig Benutzerzugänge für eine Verbindung zum Hersteller einzurichten sind. Die stellen gerade im Framework für Compliance kleinerer Unternehmen eine Herausforderung dar: Oft legen die Admins, die diese Geräte einrichten, nämlich einen generischen Zugang beim Hersteller an, der etwa ihren codierten Benutzernamen enthält („firmaxyz-maxmeier“). Und selbst wenn der Admin einen generischen Benutzernamen benutzt, kommt oft seine eigene E-Mail-Adresse zum Einsatz. Solche Details lassen sich praktisch nicht mehr auffinden, wenn der Admin das Unternehmen verlässt. Hier liegt es an der Firma, für alle Compliance-Regeln verbindlich vorzugeben, die generische Benutzernamen und die Verwendung von Mailboxen mit generischer Adresse ermöglichen.

Und die Liste lässt sich beliebig fortsetzen. Zeichnet das hauseigene Zugangssystem etwa auf, wann welche Tür geöffnet wird? Kein Problem, werden sich viele Admins denken, solange das Gerät nur aufzeichnet, dass die Tür aufgeht, aber nicht, wer sie öffnet. Anders sieht die Sache allerdings aus, wenn, um Lichter ein- und auszuschalten, im Gebäude auch smarte Bewegungsmelder zum Einsatz kommen, die ebenfalls

Aufzeichnungen führen. Aus der Information, dass um 08:05 Uhr die Türe geöffnet wurde und um 08:08 Uhr im Büro von Frau Müller das Licht anging, lässt sich aber korrelieren, dass diese vermutlich zuvor auch die Tür geöffnet hat – gerade in kleineren Unternehmen und gerade wenn das jeden Tag mit ähnlichen zeitlichen Abständen geschieht. Fans von Big Data geraten ins Schwärmen, Datenschützer hingegen ins Grübeln.

Corona lässt grüßen

Bietet das eigene Unternehmen Zugriff auf den internen Mailserver über das Internet? Gilt in der Firma gar eine BYOD-Philosophie? Wie praktisch! Gerade im Corona-Kontext und unter DSGVO-Aspekten aber alles andere als beruhigend. Denn einerseits gilt: Richtet sich ein Mitarbeiter auf einem privaten Gerät einen Zugang zu seinen Firmenmails ein, fällt dieses sofort unter dasselbe Compliance-Reglement wie alle anderen Geräte der Firma auch. Gerade weil es sich um ein privates Gerät handelt, hat die IT-Abteilung der Firma aber keine Handhabe mehr, zu bestimmen, was mit den Daten passiert. So erstrebenswert der Zugang zur Firmenmail von privaten Geräten aus auch sein mag – aus DSGVO-Sicht verbietet er sich eigentlich.

Dasselbe gilt im Corona-Kontext sogar für die Notebooks, die der Firma gehören und unter deren Compliance-Reglement stehen. Die DSGVO schreibt nämlich explizit vor, dass personenbezogene Daten so zu verarbeiten sind, dass der Zugang durch nicht berechtige Dritte unmöglich ist. Was im Büro noch umsetzbar ist, lässt sich im Homeoffice und innerhalb der eigenen vier Wände kaum rechtssicher implementieren – zumindest dann nicht, wenn kein eigener, abschließbarer Raum zur Verfügung steht. Mal eben die Mails auf dem heimischen Sofa im Wohnzimmer checken scheidet unter diesem Gesichtspunkt eigentlich aus. Dasselbe gilt analog auch für Co-Working-Spaces, in denen der Zugang zum eigenen Arbeitsplatz oft kaum einschränkbar ist.

Unternehmen sind in vielerlei Hinsicht dazu verpflichtet,

bestimmte Daten über einen langen Zeitraum hinweg vorzuhalten. Das ist im DSGVO-Kontext wie beschrieben zunächst kein Problem, weil in diesen Fällen eine andere Rechtsgrundlage besteht. Kommerzielle Lösungen, die für diese Aufgabe zum - Einsatz kommen, verfolgen jedoch das WORM-Prinzip. Sie sind hardware- wie softwareseitig um sämtliche Funktionen erleichtert, die das Modifizieren oder Löschen von Daten ermöglichen. Das wird für viele Unternehmen zum Bumerang, weil sie ihre Archive bisher nach dem Prinzip geführt haben, einfach alles zu archivieren, um sich die mühsame Arbeit des Herausfilterns der tatsächlich benötigten Elemente zu ersparen.

Archivsysteme sind ein Graus

Wer solche WORM-Konstrukte nutzt, wird ad hoc keine technische Lösung finden können, die mit vertretbarem Aufwand auch nur irgendwie realisierbar wäre. Die Deutsche Wohnen führt aus, dass das Gros der im Haus genutzten Software wie beschrieben das Löschen einzelner Dokumente aus Mieterakten aus den eben beschriebenen Gründen nicht beherrscht. Wollte man die Anbieter verpflichten, hier einzelne Teile von Datensätzen aus dem Archiv zu kratzen, müsste die Firma de facto zwei Systeme dieser Art beschäftigen: eines, in dem sie experimentell die Daten löscht, und ein zweites, in das sie dann den gültigen Datensatz überspielt, um wieder den Anforderungen an die eigene Löschpflicht zu genügen.

Archivsysteme wie dieses genügen gesetzlichen Anforderungen und geben WORM-Garantien ab, geraten damit oft aber in Widerspruch zur DSGVO (Abb. 4). *Fujitsu*

Immerhin sieht die DSGVO hier eine Hintertüre vor. Legen Unternehmen überzeugend dar, wieso der zu treibende Aufwand im Spannungsfeld von WORM-Pflichten einerseits und DSGVO-Löschpflicht andererseits zu hoch wäre, haben sie stattdessen die Option, Prozesse zu entwerfen, die verhindern, dass eigentlich zu löschende Daten wieder in Umlauf geraten. Begehren Kunden die Löschung von Datensätzen oder wäre die Löschung nötig, kann man sie dann mit einem entsprechenden Sperrvermerk versehen, der nicht zwingend im selben System hinterlegt sein muss.

Auf Verlangen muss die Firma die entsprechende Prozessdokumentation aber vorlegen können und nachweisen, dass sie in der Praxis tatsächlich zur Anwendung kommt. Und darauf verlassen, dass diese Regelung ewiglich gilt, sollten Unternehmen sich letztlich auch nicht – wer sich des Problems ernsthaft annehmen möchte, muss mit den Entwicklern etwaiger Programme zusammenarbeiten, um Datensätze sinnvoll aufteilbar zu machen. Das bedeutet am Beispiel der Deutsche Wohnen etwa ganz konkret: Die Software für die Verwaltung von Verträgen könnte die ursprünglich eingereichten Dokumente wie Gehaltsnachweise und SCHUFA-Auskünfte von sich aus sofort löschen, sobald ein Mietverhältnis in gegenseitigem Einvernehmen beendet ist. Dass es keine Option ist, das

Problem auszusitzen, zeigt das Beispiel der DW jedenfalls eindrücklich.

Ebbe bei hilfreichen Werkzeugen

Damit ist klar: Moderne IT-Umgebungen strotzen nur so vor Datensenken, die sich für Unternehmen als existenzbedrohend herausstellen können. Da ist es nur verständlich, dass Admins sich Werkzeuge wünschen, die ihnen beim Auffinden der Datentröge helfen und gegebenenfalls Alarm schlagen. Die schlechte Nachricht ist: Solche Tools sind kaum verfügbar. Werkzeuge zur forensischen Analyse beziehen sich eher auf Fälle, in denen ein Einbruch stattgefunden hat und Daten - bereits rausgetragen worden sind. Das ist im DSGVO-Kontext aber nur dann schädlich, wenn die Firma nicht nachweisen kann, dass sie sich an aktuelle technische Standards beim Absichern der eigenen Umgebung gehalten hat.

Dataloss Prevention Tools zäumen das Pferd von hinten auf und sind eher darauf ausgelegt, Prozesse zu installieren, die Datenverlust unwahrscheinlich machen. Das hilft aber nicht in bestehenden Umgebungen, in denen Grundsätze des Datenschutzes über Jahre hinweg nicht zur Anwendung gekommen sind.

Was können Unternehmen also tun? Wie bereits angedeutet, ist die richtige Reaktion auf die DSGVO-Löschpflicht in erster Linie die Einführung passender Prozesse in Kombination mit ausgiebiger Kommunikation mit den eigenen Lieferanten. Standardisierung, Automation und Orchestrierung nehmen viel Angriffsfläche. Überraschenderweise existiert mit der DIN 66398 sogar eine recht praxisorientierte Norm zu diesem Thema (siehe Kasten „Löschkonzepte gemäß DIN 66398“).

Löschkonzepte gemäß DIN 66398

Das DIN hat in der DIN 66398 Empfehlungen als „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ zusammengestellt. Darin finden

sich für das Normungsinstitut ungewöhnlich konkrete Vorgaben zur Vorgehensweise beim Erstellen eines Löschkonzepts.

In einem Blog des Forum-Verlags heißt es, dass demnach Unternehmen eine Reihe von Überlegungen anstellen und Schritte unternehmen sollten (siehe ix.de/z9h2):

- Datenarten, die es im Unternehmen gibt, kategorisieren und deren Aufbewahrungsfristen festlegen.
- Löschregeln für die jeweilige Datengruppe festlegen.
- Konkrete Umsetzungsregeln definieren.
- Die jeweils verantwortlichen Personen für die datenschutzkonforme Umsetzung benennen.
- Prozesse zur Dokumentation ausarbeiten und verbindlich festlegen.

Automation und Orchestrierung

Wer sein Set-up sinnvoll automatisiert und modernen Standards der Systemadministration folgt, minimiert das Risiko von Datensenken auf einzelnen Servern. Überhaupt sollte ein einzelnes System so wenige personenbezogene Daten enthalten wie möglich. Was im Klartext bedeutet: Sämtliche Benutzerzugänge der Systeme kommen aus dem LDAP. Der Prozess des Offboardings sieht Schritte vor, die Daten ehemaliger Kollegen auf Systemen zentralisiert und automatisiert zu entfernen, sofern diese für den Betrieb nicht nötig sind. Logdateien haben in modernen Systemen auf einzelnen Servern nichts mehr zu suchen. Zentralisiertes Logging ist stattdessen das Zauberwort – und ermöglicht es, zentral der DSGVO-Löschpflicht nachzukommen, zum Teil sogar vollständig automatisch.

Was spezielle Software wie Shopsoftware oder Vertragsverwaltungslösungen angeht, hilft nur die enge Kommunikation mit dem Hersteller. Falls der sein Produkt bisher nicht um eine Löschfunktion nach DSGVO-Standards erweitert hat, gilt es, Druck auszuüben, um das zu ändern.

Sich darauf zu verlassen, dass der „Machbarkeitsvorbehalt“ in der DSGVO dauerhaft erhalten bleibt, ist jedenfalls eine fragwürdige Strategie. Hier muss die Software a priori die Möglichkeit bieten, Daten eines Profils zu löschen, ohne dieses gleich vollständig aus dem Bestand zu entfernen.

Den Verheißungen des Internet of Things sollten Unternehmen vom Standpunkt der DSGVO her derzeit widerstehen. Smarte Lichtschalter und schlaue Kaffeemaschinen sind zwar bequem und angenehm. Doch sind sie zentral kaum administrierbar – und sie lassen sich nicht in automatisierte Compliance-Frameworks einbinden und werden so zum potenziellen Datentrog.

Fazit

Es ist eine Krux mit dem Datenschutz: Zu Recht formuliert die DSGVO ein hohes Recht der Menschen an den eigenen Daten, der besonderen Schutzbedürftigkeit dieser Daten und eine Verpflichtung für Daten verarbeitende Unternehmen, hohe Standards zu erfüllen. Für die Admins im Unternehmen geht das aber derzeit mit weitgehend unabwägbaren Risiken einher: In den wenigsten Firmen dürfte wirklich klar sein, wo sich möglicherweise noch alte Bestandsdaten verbergen, die längst den Weg in die ewigen Jagdgründe hätten antreten müssen. Wer jedoch diese Datensätze konsequent suchen und heben möchte, kommt um ein nahezu vollständiges Audit des eigenen Set-ups kaum herum. Und das behebt nur einen Teil der Schwierigkeiten.

Denn verschiedene Softwarelösungen und Archivimplementierungen, ganz gleich, ob in Hard- oder Software umgesetzt, verunmöglichen es, die Löschregeln der DSGVO in Gänze einzuhalten. Hier dürfte zumindest auf absehbare Zeit eine sehr enge Abstimmung mit dem eigenen Rechtsbeistand notwendig sein, um die Grenzen des Erlaubten zu kennen und sich an ihnen entlangzuhangeln. Aber langfristig muss die DSGVO zur Vereinheitlichung und Standardisierung von Set-ups im Rechenzentrum führen, weil sich damit viele Komplikationen im Hinblick auf Datenschutz von vornherein

vermeiden lassen.
(avr@ix.de)

1. Quellen
2. Tobias Haar; Seid sparsam; Löschung personenbezogener Daten; *iX* 11/2020, S. 58
3. Frank Heisel; Ballast abwerfen; Datenlöschen in komplexen Systemlandschaften; *iX* 11/2020, S. 64
4. Weitere Informationen zu Datenempfängern und zur DIN 66398: ix.de/z9h2

Martin Gerhard Loschwitz

ist Cloud Platform Architect bei Drei Austria und beackert dort Themen wie OpenStack, Kubernetes und Ceph.

[/expand]