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]