Löschpflichten

DSGVO-konformes Löschen und Vernichten von Daten

TKMmedia DATENSCHUTZ

Inhaltsverzeichnis

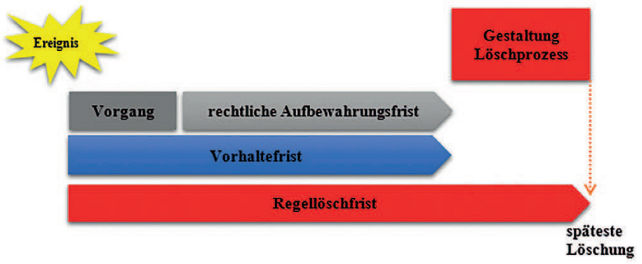
Löschkonzepte: So gehen Sie konkret vor

In zahlreichen Unternehmensprozessen werden personenbezogene Daten verarbeitet und genutzt. Diese personenbezogenen Daten unterliegen den gesetzlichen Anforderungen des Datenschutzes und damit den Prinzipien der Erforderlichkeit, Datenvermeidung und Datensparsamkeit, die auch eine Löschung personenbezogener Daten notwendig machen. In Art. 17 der EU-Datenschutz-Grundverordnung (DSGVO) wird das Recht auf Löschung („Recht auf Vergessenwerden") geregelt. Für Sie als Datenschutzbeauftragten ist es jetzt eine zentrale Aufgabe, in Ihrem Unternehmen zu prüfen, ob für alle personenbezogenen Daten sachgerechte Löschkonzepte vorliegen.

Datenbestand, Vorhaltefrist, Regellöschfrist: Das müssen Sie wissen

Als Datenschutzbeauftragter sollten Sie zunächst feststellen, welche personenbezogenen Daten in Ihrem Unternehmen verarbeitet werden. Wird ein vollständiges Verzeichnis der Verarbeitungstätigkeiten geführt, können Sie die Informationen daraus entnehmen. Zur Ausarbeitung von Löschkonzepten hat es sich bewährt, den Datenbestand des Unternehmens in Datenkategorien und Datenobjekte einzuteilen. Ein Datenobjekt ist eine Sammelbezeichnung für Objekte wie z. B. Dateien, Dokumente, Datensätze oder Attribute. Datenobjekte und damit auch Datenkategorien können an verschiedenen Speicherorten abgelegt sein.

Für jede Datenkategorie ist zu klären, wie lange sie in den Geschäftsprozessen benötigt wird. Datenkategorien müssen aufgrund fachlicher Anforderungen sowie gesetzlicher Aufbewahrungspflichten verfügbar sein. Hieraus ergibt sich die Vorhaltefrist. Hauptansatz ist die Anwendung von Standardfristen, die sich primär aus Rechtsvorschriften ergeben. Ist nur allgemein die Lösch-Erforderlichkeit gegeben, sind Standardlöschfristen anhand von einfach zu haltenden Kriterien abzuleiten. Beispiele hierfür sind eine sofortige Löschung (z. B. § 13 Abs. 4 Satz 1 Nr. 2 Telemediengesetz (TMG)) oder ein Vorhaltefrist gemäß Art. 5 Abs. 1e DSGVO.



Wenn eine Vorhaltefrist endet, greift für personenbezogene Daten die allgemeine Löschpflicht (z. B. aus Art. 5 Abs. 1e DSGVO), wonach die Daten nach Wegfall der Erforderlichkeit zur Zweckerfüllung zu löschen sind. Aus der Vorhaltefrist zzgl. der für die technische Umsetzung der Löschung vorgesehenen Zeit (Gestaltung des Löschprozesses) ergibt sich die Regellöschfrist eines Datums. Existiert eine gesetzlich streng vorgeschriebene Höchstspeicherfrist, muss der Vorgang des Löschens bis zum Ablauf dieser Frist abgeschlossen sein. Hier stimmen dann Höchstspeicherfrist und Regellöschfrist überein.

Löschung, Einschränkung und Anonymisierung: Diese Definitionen müssen Sie kennen

Als Löschung wird die unwiderrufliche Vernichtung bzw. Unkenntlichmachung der Datenobjekte (Daten oder Datenträger) definiert. Gemäß Art. 17 DSGVO ist das Löschen auf Anforderung definiert; hiernach kann die betroffene Person eine unverzügliche Löschung durch den Verantwortlichen verlangen, sofern

- der Zweck für die Datenverarbeitung entfallen ist,
- die ermächtigende Einwilligung widerrufen wurde oder
- die Datenverarbeitung unrechtmäßig erfolgt ist.

Gemäß Art. 18 DSGVO kann die betroffene Person die Einschränkung der Verarbeitung vom Verantwortlichen verlangen, sofern für die Dauer der Prüfung bei der durch den Betroffenen bestrittenen Richtigkeit der Daten

- die Datenverarbeitung unrechtmäßig erfolgt ist und eine Löschung durch den Betroffenen nicht verlangt wird,

- der Zweck für die Datenverarbeitung entfallen ist und eine Löschung durch den Betroffenen aufgrund von Rechtsanspruchssicherungen nicht verlangt wird oder
- im Rahmen der Widerspruchseinlegung (Art. 21 Abs. 1 DSGVO) die Interessensabwägung bzgl. der berechtigten Gründe noch nicht abgeschlossen ist.

WICHTIG: Die Anonymisierung ist die Veränderung personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können. Bei der Anonymisierung ist zwingend zu beachten, dass nur eine absolute Anonymisierung eine Löschung ersetzen kann.

Löschkonzepterstellung: Das ist zu tun
Die Löschung von Daten muss der Prozessverantwortliche sicherstellen.
Es muss festgelegt werden,

- welche Löschregeln für welche Datenbestände gelten,
- wie aus den Löschregeln die Datenlöschung in Prozessen erreicht wird (z. B. manuell, automatisiert);
- Mindestanforderung an die Dokumentation der Löschregeln, Umsetzungsvorgaben und durchgeführten Löschmaßnahmen
- Verantwortlichkeiten für die entstehenden Aufgaben der Umsetzung, Überprüfung und Fortschreibung (inkl. Fehlerbehandlung und mögliche Sonderfälle) Diese Festlegungen bilden dann das jeweilige Löschkonzept.

FAZIT:
Die Datenlöschung ist ein komplexer Prozess und sollte zumindest nach folgenden Regeln praktiziert werden:

- Daten sind nicht zufällig, sondern nach sinnvollen Regeln zu löschen.
- Es sind datenschutzkonforme Löschregeln zu definieren.
- Rechtliche Aufbewahrungspflichten sind Teil des Verwendungsprozesses und damit der Aufbewahrungsfrist.

Richtig beraten: So klappt es mit Lösch-, Sperr- und Aufbewahrungsfristen

Stellen Sie sich vor, Sie werden von einem Mitarbeiter gefragt, wie lange etwa die personenbezogenen Daten zu Kundenbestellungen gespeichert beziehungsweise wann diese gesperrt oder gelöscht werden müssen. Weil man sich datenschutzkonform verhalten will, sollen Sie bei der Findung der richtigen Fristen unterstützen. Doch was können Sie raten? Nachfolgend finden Sie die wichtigsten Fälle dargestellt. Prüfen Sie, welcher Fall auf den Ihnen geschilderten Sachverhalt beziehungsweise die infrage stehenden personenbezogenen Daten zutrifft.

Fall 1: Unzulässig verarbeitete personenbezogene Daten (Art. 17 Abs. 1 lit. d DSGVO)
Sind personenbezogene Daten ohne tragfähige Rechtsgrundlage verarbeitet worden, dürfen diese weder weiter gespeichert noch sonst wie genutzt werden. Sie sind unverzüglich zu löschen.

Fall 2: Personenbezogene Datenwerden für berechtigte Interessen des Verantwortlichen verarbeitet (Art. 6 Abs. 1 lit. f DSGVO)
Hier sind 2 Unterfälle zu unterscheiden:

Variante A: Die Kenntnis der für berechtigte Interessen verarbeiteten Daten ist für die Erfüllung des Zwecks der Verarbeitung weiterhin erforderlich. Dies hat zur Folge, dass die Daten weiterhin verarbeitet werden dürfen.

Variante B: Die Kenntnis der für berechtigte Interessen verarbeiteten Daten ist für die Erfüllung des Zwecks der Verarbeitung nicht mehr erforderlich. Dies hat zur Folge, dass die Daten eigentlich zu löschen wären. Sofern Aufbewahrungspflichten bestehen, dürfen die Daten jedoch nicht gelöscht werden (vgl. Art. 17 Abs. 3 lit. b DSGVO). Sie sind dann einzuschränken, sprich, sie sind zu kennzeichnen, damit ihre weitere Verarbeitung eingeschränkt wird.

> **Tipp:** Als Aufbewahrungspflichten kommen insbesondere solche nach dem Steuerrecht (z. B. § 147 Abgabenordnung) oder Handelsrecht (§ 257 Handelsgesetzbuch) in Betracht. Je nachdem, um welches Dokument es sich handelt, besteht eine Aufbewahrungspflicht von 6 oder 10 Jahren.

Fall 3: Eine Betriebsvereinbarung regelt das Löschen, Sperren oder Aufbewahren
Kollektivvereinbarungen wie Betriebsvereinbarungen gelten als Rechtsgrundlage im Sinne des Art. 88 DSGVO und können die Verarbeitung personenbezogener Daten in den Anwendungsbereich der Betriebsvereinbarung fallender Arbeitnehmer regeln. Finden sich in einer einschlägigen Betriebsvereinbarung Festlegungen zum Löschen, Sperren oder Aufbewahren personenbezogener Daten, so sind diese vorrangig zu berücksichtigen und anzuwenden, sofern sie die Regelungen der DSGVO unterschreiten.

Fall 4: Personenbezogene Daten werden für fremde Geschäftszwecke verarbeitet
Es kann auch vorkommen, dass Ihr Unternehmen Daten für fremde Zwecke verarbeitet, z. B. im Rahmen einer sogenannten Datenverarbeitung im Auftrag (Art. 28 DSGVO). In einem solchen Fall unterliegt Ihr Unternehmen den Weisungen des Auftraggebers. Auftraggeber und Auftragnehmer sind bei der Datenverarbeitung im Auftrag für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Das gilt auch für das Thema Löschen und Sperren personenbezogener Daten. Findet sich in einer schriftlichen Vereinbarung keine Festlegung dazu, wann die im Auftrag verarbeiteten Daten zu löschen oder zu sperren sind, sollten Sie diese Festlegung vom Auftraggeber einfordern. Die Umsetzung der Festlegung in der Praxis kommt natürlich Ihrem Unternehmen als weisungsgebundenem Auftragnehmer zu.

Problem Löschdokumentation: Denken Sie an diese praktikablen Lösungen

Vielleicht hatten Sie auch schon einmal das folgende Problem: Das Löschen von Daten an sich stellt eigentlich kein Problem dar, weil etwa die geeignete Software zum Löschen vorhanden ist.Doch wie lässt sich dokumentieren, dass eine Löschung stattgefunden hat, wenn beispielsweise die Löschsoftware kein Protokoll erzeugt oder dieses nicht ausgedruckt werden kann?

Besonders mit Blick auf Art. 17 DSGVO (Recht auf Löschung) ist es wichtig, der betroffenen Person die Löschung nachweisen zu können. Hier sollten Sie praktisch denken und etwa eine dieser Möglichkeiten zum Einsatz bringen:

- **Schriftliche Dokumentation**

Halten Sie schriftlich fest, welche Daten Sie wann, mit welcher Software und auf welche Weise (z. B. Löschschema, Anzahl Überschreibvorgänge) gelöscht haben. Denken Sie daran, den zu löschenden Gegenstand möglichst konkret zu beschreiben; bei Festplatten reichen der Hersteller und die Seriennummer.

- **Fotodokumentation**

Wie heißt es so schön: Ein Bild sagt mehr als tausend Worte. Einen geeigneten Löschnach- weis können Sie auch erbringen, indem Sie einige Fotos mit der Digitalkamera machen. 3 Fotos reichen in der Regel

aus: eines zu Beginn des Löschvorgangs, eines während der Löschung und eines zum Schluss. Legen Sie diese Bilder unverändert ab und entfernen Sie nicht die automatisch gespeicherten Bildinformationen, die sogenannten EXIF-Daten. Diese enthalten nämlich zusätzlich Datum, Uhrzeit und ggf. sogar die GPS-Koordinaten der Aufnahmen.

Ausgeschiedene Mitarbeiter: Diese Daten muss Ihr Unternehmen löschen

Mitarbeiter kommen und gehen. Das ist eigentlich nichts Außergewöhnliches. Doch mit Verlassen des Unternehmens kommt oft die Frage auf: Welche Daten müssen gelöscht und welche aufgehoben werden? Geben Sie aus Ihrer datenschutzrechtlichen Sicht diese Tipps!

Davor, währenddessen und danach
Im Laufe eines Beschäftigtenverhältnisses kommen eine Menge personenbezogene Daten zusammen. Angefangen bei den Bewerbungsunterlagen mit Anschreiben, Lebenslauf und Zeugnissen bis hin zu Kontaktdaten, Bankverbindungen sowie besonders sensiblen Informationen wie Gesundheitsdaten – mit der Zeit sammelt sich so einiges an.

Als verantwortliche Stelle muss sich Ihr Unternehmen beim Umgang mit den personenbezogenen Daten seiner Beschäftigten an datenschutzrechtliche Regelungen und Grundsätze halten. Das heißt, es muss dafür sorgen, dass es mit personenbezogenen Daten datenschutzkonform umgeht, sie sicher aufbewahrt und unbefugten Personen nicht zur Kenntnis gelangen können.

Löschen von Daten
Ein Datenschutzgrundsatz spielt dabei eine besondere Rolle. Er ist in §35 Abs. 2 Satz 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) verankert und besagt, dass personenbezogene Daten zu löschen sind, wenn der Zweck, für den sie erhoben wurden, entfällt. Dieser Grundsatz gilt auch mit Geltungsbeginn der Datenschutz-Grundverordnung (DSGVO) am 25.5. weiter.

Die entsprechende Regelung ist in Art. 17 Abs. 1 Buchst. a DSGVO zu finden. Fällt der Zweck also weg, weil der Mitarbeiter das Unternehmen verlässt,
muss die Personalabteilung prüfen, welche Daten sie löschen muss.

Ausnahmen von der Löschung
Machen Sie stets deutlich: Verlässt ein Mitarbeiter das Unternehmen, dürfen keinesfalls seine Daten einfach gelöscht werden. Denn der Löschpflicht steht eine Reihe von Regelungen gegenüber, die für bestimmte Daten eine Aufbewahrungsfrist vorsehen. So z. B. können Aufbewahrungsfristen oder die schutzwürdigen Interessen des Betroffenen einer Löschung entgegenstehen. In diesen Fällen ist gemäß § 35 Abs. 3 BDSG nicht die Löschung, sondern die Sperrung der Daten vorzunehmen.

Tipp: Lassen Sie in Ihre Beratung einfließen, dass die Kollegen in der Personalabteilung nicht nur beim Löschen, sondern auch beim Sperren der Daten geeignete technische und organisatorische Maßnahmen ergreifen müssen, damit kein Unbefugter die Daten mehr verwenden kann. In der DSGVO sind die Ausnahmen von der Löschpflicht in Art. 17 Abs. 3 verankert.

Ob zukünftig auch ein Sperren personenbezogener Daten noch zulässig ist, wenn etwa das Löschen mit unverhältnismäßigem Aufwand verbunden wäre, ist umstritten. Aus der DSGVO lässt sich das nicht ableiten. Diese kennt nur das Löschen.

Nicht übersehen: Unternehmensspezifische Regeln
Neben gesetzlichen Regelungen können aber auch auf Ihr Unternehmen zugeschnittene Aufbewahrungs- oder Löschpflichten bestehen. Vielleicht gibt es dazu Betriebsvereinbarungen in Ihrem Unternehmen, die die Kollegen dann berücksichtigen müssen. Diese müssen folgerichtig auch tatsächlich umgesetzt sein.

Nehmen Sie diese Brennpunkte unter die Lupe
Verlässt ein Mitarbeiter das Unternehmen, sind besonders an folgenden Orten personenbezogene Daten zu finden, die auf Löschen, Sperren oder Aufbewahren zu prüfen sind:

Brennpunkt 1: Personalakte
In der Personalakte sind vielfältige personenbezogene Daten enthalten. Dabei kommt es nicht darauf an, ob die Daten in elektronischer Form oder in Papierform vorliegen – in beiden Fällen gelten die datenschutzrechtlichen Bestimmungen. Ihr Unternehmen als verantwortliche Stelle ist verpflichtet, die Personalakten sicher aufzubewahren, das heißt, vor Kenntnisnahme durch Unbefugte zu schützen. Besonders sensible Informationen nach § 3 Abs. 9 BDSG bzw. Art. 9 DSGVO sind auch durch entsprechende Maßnahmen besonders zu schützen und vertraulich zu behandeln. Einsicht in die Personalakte darf nur ein möglichst kleiner Kreis von Personen haben. Jeder Beschäftige kann die vorhandenen Daten in seiner eigenen Personalakte prüfen und falsche Daten löschen, sperren oder berichtigen lassen.

> **ACHTUNG:** Je nach Inhaltstyp der Personalakte können unterschiedliche Aufbewahrungspflichten bestehen. Unter Umständen müssten Teile früher gelöscht werden. Welche Aufbewahrungspflichten bestehen, sollten Sie gemeinsam mit der Personalabteilung klären. Sie müssen diese nicht allein festlegen.

Brennpunkt 2: E-Mail-Postfach
Grundsätzlich gilt: Ein Mitarbeiter sollte das Unternehmen nicht verlassen, ohne vorher sein E-Mail-Fach auf persönliche bzw. private E-Mails zu überprüfen und diese ggf. zu löschen. Die geschäftliche Korrespondenz wird an den Nachfolger oder Vorgesetzten weitergegeben. Ist die E-Mail-Nutzung in Ihrem Unternehmen lediglich zu betrieblichen Zwecken gestattet und die private Nutzung ausdrücklich verboten, können die E-Mails prinzipiell auch automatisch an ein anderes E-Mail-Postfach weitergeleitet werden. Um allen Eventualitäten vorzubauen, ist es jedoch in der Praxis besser, Geschäftliches weiterzugeben, das Postfach zu schließen und unverzüglich durch die zuständige Abteilung deaktivieren zu lassen.

Datenträgerlöschung: Sensibilisieren Sie Ihre Mitarbeiter!

Auch wenn es sich eigentlich schon längst herumgesprochen haben sollte, so zeigen manche Pressemeldungen, dass Datenträger mit personenbezogenen Daten nicht in jedem Fall ordnungsgemäß entsorgt werden. Immer wieder tauchen etwa bei eBay oder schlichtweg im Müll Festplatten und andere Datenträger von Unternehmen auf, die wegen der nicht gelöschten Daten deren ehemalige Besitzer ganz schön in die Bredouille bringen. Finden sich etwa personenbezogene Daten auf den Datenträgern, lässt sich ein Verstoß gegen den Datenschutz nicht mehr bestreiten. Dem können auch Sie als Datenschutzbeauftragter vorbeugen, indem Sie die Mitarbeiter für das Thema Datenlöschung sensibilisieren.

Praxisnah können Sie dies etwa mit einem Merkblatt bewerkstelligen, das Sie im Intranet veröffentlichen oder etwa an die Mitarbeiter per E-Mail versenden. Orientieren Sie sich doch an diesem Beispiel:

Merkblatt: Sichere Löschung von Datenträgern -Darauf sollten Sie achten

Sehr geehrter Mitarbeiter,

egal, ob es sich um personenbezogene Daten oder andere schutzwürdige Informationen des Unternehmens handelt, bitte tragen Sie dazu bei, dass diese nicht in falsche Hände geraten. Schließlich kann ein entsprechender Datenschutzverstoß ein erhebliches Bußgeld nach sich ziehen. Aber auch das Image unseres Unternehmens kann stark in Mitleidenschaft gezogen werden.

Wenn es um das Löschen von Daten und Datenträgern geht, bitte beachten Sie folgende grundsätzliche Hinweise:

Formatieren reicht nicht
Wenn Sie einen Datenträger (z.B. Festplatte, USB oder Speicherstick) lediglich formatieren, sind die Daten nur auf den ersten Blick gelöscht. Die Daten sind nach wie vor vorhanden. Es wird quasi nur das „Inhaltsverzeichnis" entfernt, die Daten an sich bleiben jedoch unberührt. Dass das keine sichere Datenlöschung sein kann, erkennen Sie, wenn Sie den Vergleich zu einem Buch ziehen. Fehlt das Inhaltsverzeichnis, sind dennoch alle Informationen weiter verfügbar. Gehen Sie daher lieber auf Nummer sicher und lassen Sie durch eine Software die Daten mit Nullen und Einsen überschreiben.

Je sensibler Informationen, desto häufiger sollten Sie überschrieben werden
Früher ging man davon aus, dass Daten erst dann sicher gelöscht sind, wenn sie mindestens 7fach mit einem zufälligen Muster aus Nullen und Einsen überschrieben wurden. Doch je großer das Speichermedium ist und je mehr Überschreibvorgänge durchgeführt werden, desto länger dauert das Ganze. Wissenschaftliche Untersuchungen haben gezeigt, dass es in der Regel ausreichend ist, wenn Datenträger einmalig mit Nullen und Einsen überschrieben werden. Bei manchen Daten sollten Sie jedoch lieber auf Nummer sichergehen. Befinden sich auf einem Datenträger etwa besonders sensible und schadensträchtige Informationen (insbesondere Daten im Sinne von Art. 9 DSGVO wie etwa Gesundheitsdaten) ist das mehrfache Überschreiben des Datenträgers vorzuziehen. Dabei reicht ein 3faches Überschreiben aus. Bei der Auswahl geeigneter Löschsoftware stehen Ihnen IT-Abteilungen und Datenschutzbeauftragte zur Verfügung.

Defekte und veraltete Speichermedien nicht einfach wegwerfen
Es kann durchaus passieren, dass Sie an einen Datenträger geraten, der defekt zu sein scheint oder der schon so veraltet ist, dass Sie diesen überhaupt nicht mehr anschließen und lesbar machen können. Das bedeutet allerdings nicht, dass niemand mehr diese Möglichkeit hat. Werfen Sie defekte oder veraltete Datenträger nicht vorschnell weg. Fragen Sie lieber bei der IT-Abteilung und beim Datenschutzbeauftragten nach, wie damit umgegangen werden soll. Einen Weg zur sicheren Datenlöschung gibt es immer. So können defekte Festplatten beispielsweise durchbohrt oder beim Dienstleister mittels eines sogenannten Degaussers entmagnetisiert werden.

Denken Sie auch an moderne Speichermedien
Nicht nur Festplatten, Disketten und Datenbänder können schützenswerte Informationen enthalten und sollten sicher gelöscht werden. Denken Sie auch an andere Speichermedien (z.B. in Digitalkameras) oder Smartphones, CDs, …

Achten Sie bereits bei der Beschaffung auf Löschmöglichkeiten
Daten sicher zu löschen ist heutzutage wichtiger denn je. Fast alle modernen Geräte, auch Kopierer und Faxgeräte, speichern unzählige Informationen. Achten Sie bereits bei der Beschaffung darauf, wie bei solchen Geräten Daten gelöscht werden können und geben Sie Geräten den Vorzug, die Ihnen die Umsetzung dieser wichtigen Datenschutzanforderung auf einfache Weise ermöglichen.

Unterstützen Sie auch Kollegen
Sollten Sie einmal mitbekommen, wie ein Kollege einen Datenträger im Mülleimer entsorgt, fragen Sie diesen ruhig, ob dieser Entsorgungsweg wohl der Richtige ist. Schon ein kurzes Gespräch unter Kollegen kann dazu beitragen, dass Daten nicht in falsche Hänge geraten, das Unternehmen nicht in die Schlagzeilen gerät und sogar Arbeitsplätze auf dem Spiel stehen.

Fragen kostet nichts
Lieber auf Nummer sichergehen: handeln Sie nach diesem Motto, wenn Sie in Sachen Löschung von Daten mit Ihrem Latein am Ende sind oder sich schlichtweg unsicher sind, wie richtig vorzugehen ist. Sprechen Sie die IT-Abteilung oder mich, Ihren Datenschutzbeauftragten, an. Gemeinsam werden wir eine Lösung finden.

Ihr Datenschutzbeauftragter

Löschung und Einschränkung: Antworten auf die wichtigsten Fragen Ihrer Kollegen

Ein wichtiger Grundsatz des Datenschutzes ist, dass einmal verarbeitete personenbezogene Daten nicht für immer und ewig gespeichert werden dürfen, weil man sie eventuell ja noch mal für irgendeinen Zweck brauchen könnten.

Eine solche Datenspeicherung auf Vorrat soll durch die Pflicht zur Löschung und Einschränkung der Verarbeitung personenbezogener Daten verhindert werden. Wenn Sie sich selbst mit dem Thema Löschung und Einschränkung beschäftigen oder Mitarbeitern die wesentlichen Grundsätze vermitteln wollen, tauchen immer wieder dieselben Fragen auf. Damit Sie nicht kalt erwischt werden, finden Sie hier Antworten auf neun häufig gestellte Fragen.

1. Wo sind die Themen Löschung und Einschränkung der Verarbeitung personenbezogener Daten geregelt?
Wann welche personenbezogenen Daten auf welche Art und Weise zu löschen oder einzuschränken sind, kann an vielen Orten geregelt sein. So kann etwa eine Betriebsvereinbarung Vorgaben zu personenbezogenen Daten machen, welche die Mitarbeiter des Unternehmens betreffen. In der DSGVO widmen sich in erster Linie Art. 17 der Löschung und Art. 18 der Einschränkung der Verarbeitung personenbezogener Daten. Neben den Festlegungen der DSGVO und des BDSG-neu (§ 35) können auch andere Gesetze Festlegungen treffen. So finden sich etwa im Telekommunikationsrecht oder im Steuerrecht (z. B. § 147 Abgabenordnung) genauso Regelungen, aus denen sich Fristen zu Aufbewahrung und Löschung von Daten ableiten.

2. Was bedeutet Löschen?
Gemäß § 3 Abs. 4 Nr. 5 BDSG ist unter Löschen das Unkenntlich machen gespeicherter personenbezogener Daten zu verstehen. Bei Datenträgern erfolgt das Unkenntlich machen beispielsweise durch mehrfaches Überschreiben oder durch Zerstören des Datenträgers. Bei Dokumenten in Papierform kann das Unkenntlich machen durch Schreddern erfolgen. Allerdings muss beim Löschen immer eines gewährleistet sein: Das Löschen muss unumkehrbar sein, sprich, einmal gelöschte Daten dürfen nicht wiederherstellbar sein.

Tipp: Das Schwärzen von Informationen in Papierunterlagen ist zwar durchaus auch als geeignete Maßnahme zum Löschen personenbezogener Informationen anerkannt. Doch häufig ist die Information nur auf den ersten Blick unkenntlich gemacht, weil sie etwa mit einem schwarzen Stift übermalt wurde. Halten Sie das geschwärzte Dokument doch einfach einmal gegen das Licht. Nicht selten wird das Geschwärzte lesbar sein.

3. Wann müssen personenbezogene Daten gelöscht werden?
Grundsätzlich müssen personenbezogene Daten gelöscht werden, wenn für deren Speicherung keine Rechtsgrundlage bestand oder diese Rechtsgrundlage nichtmehr besteht. Wurden personenbezogene Daten ohne Rechtsgrundlage erhoben, weil beispielsweise in einem Formular unzulässige Informationen abgefragt wurden, dann müssen die Daten gelöscht werden. Auch kann eine Rechtsgrundlage später wegfallen. Die Rechtsgrundlage besteht etwa dann nicht mehr, wenn eine Einwilligung in die Verarbeitung personenbezogener Daten widerrufen wurde. Der Wegfall der Rechtsgrundlage führt dazu, dass die entsprechenden Informationen gelöscht werden müssen.

Personenbezogene Daten müssen auch dann gelöscht werden, wenn der Zweck ihrer Speicherung erreicht wurde und daher ihre Kenntnis für die Erreichung des Zwecks nicht mehr erforderlich ist (Art. 17 Abs. 1 lit. a DSGVO). Allerdings kann es passieren, dass diese eigentlich zu löschenden personenbezogenen Daten nicht gelöscht werden dürfen, weil etwa gesetzliche Regelungen eine Aufbewahrung vorschreiben. In einem solchen Fall tritt an die Stelle der Löschung der Daten die Einschränkung der Verarbeitung.

Tipp: In Art. 17 DSGVO ist nur festgelegt, dass personenbezogene Daten bei Vorliegen bestimmter Voraussetzungen zu löschen sind. Auch wenn kein Zeitraum genannt wurde, muss davon ausgegangen werden, dass das Löschen unverzüglich zu erfolgen hat. Unverzüglich bedeutet „ohne schuldhaftes Zögern", sprich, in Anbetracht der Umstände des Einzelfalls so schnell wie möglich.

4. Muss dokumentiert werden, dass personenbezogene Datengelöscht wurden?
Zwar ist die Dokumentation der Löschung von personenbezogenen Daten nicht gesetzlich vorgeschrieben, allerdings kann eine Dokumentation im Fall der Fälle die Beweisführung erleichtern, dass bestimmte personenbezogene Daten zu einem bestimmten Zeitpunkt gelöscht wurden. Wird Ihr Unternehmen etwa durch ein anderes Unternehmen mit der Verarbeitung personenbezogener Daten beauftragt (sogenannte Auftragsverarbeitung nach Art. 28 DSGVO), muss Ihr Unternehmen nach Abschluss des Auftrags auch belegen können, dass die im Auftrag verarbeiteten Daten auch wieder gelöscht wurden. Das ist dann besonders wichtig, wenn personenbezogene Daten in unberechtigte Hände gelangt sein sollten. Hatte Ihr Unternehmen die Datenschon vorher ordnungsgemäß gelöscht und kann es dies belegen, scheidet Ihr Unternehmen als Verursacher aus.

5. Was ist unter Einschränkung der Verarbeitung zu verstehen?
Der Gesetzgeber hat in Art. 4 Nr. 3 DSGVO den Begriff definiert: Die „Einschränkung der Verarbeitung" ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Im Gegensatz zum Löschen ist das Sperren reversibel. Das heißt, die gesperrten personenbezogenen Daten können entsperrt, sprich wieder les- und nutzbar gemacht werden.

6. Wie kann die Verarbeitung personenbezogener Daten eingeschränkt werden?
In der DSGVO wurde nicht konkret festgelegt, in welcher Weise die Verarbeitung personenbezogener Daten einzuschränken ist. Insofern kommt das Auslagern von Daten oder Akten in einen verschlossenen Schrank oder einen anderen Raum genauso in Betracht wie das Auslagern der elektronisch gespeicherten Daten in einen anderen Speicherbereich beziehungsweise das Speichern auf einer Daten-CD oder externen Festplatte. Aber auch durch das Verändern von Zugriffsberechtigungen können personenbe-

zogene Daten in einer Datenbank oder einem CRM-System der weiteren Verarbeitung oder Nutzung entzogen werden. Auch mit dem Verschlüsseln von Daten können diese gesperrt werden. Werden Adressen z. B. bei einem Adresshändler eingekauft, empfiehlt es sich, die gesperrten Datensätze in einer gesonderten Sperrdatei zu speichern. Der Import neuer Daten wird dann gegen die Sperrdatei geführt, um auszuschließen, dass bereits gesperrte Adressen neu aufgenommen werden.

7. Was passiert, wenn der Lösch- oder Einschränkungspflicht nicht entsprochen wird?

Neben Speichern, Verändern und Übermitteln sind auch das Einschränken und Löschen personenbezogener Daten Ausprägungen der Verarbeitung personenbezogener Daten. Werden zu löschende Daten nicht gelöscht, werden sie zwangsläufig weiterhin gespeichert. Weil dies unzulässig ist, können die Aufsichtsbehörden eine Geldbuße verhängen. Dies ergibt sich aus Art. 83 Abs. 5 lit. b. Ein Verstoß gegen die Rechte der betroffenen Person (z. B. Art. 17 DSGVO) kann demnach mit einer Geldbuße von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden, je nachdem, welcher der Beträge höher ist. Weiterhin können die Mitgliedsstaaten der EU Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung festlegen – insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 DSGVO unterliegen. Diese Sanktionen müssen ebenso wie die Geldbußen wirksam, verhältnismäßig und abschreckend sein.

8. Dürfen eingeschränkte personenbezogene Daten wieder zur Verarbeitung freigegeben werden?

Ziel der Einschränkung der Verarbeitung ist es u. a. zu löschende Daten, die z. B. aus steuerrechtlichen Gründen aufbewahrt werden müssen, der Datenverarbeitung zu entziehen. Aber es gibt auch Fälle, in denen gesperrte Daten genutzt oder an Dritte weitergegeben werden dürfen. Dies ist nach Art. 18 Abs. 2 etwa der Fall, wenn Folgendes gegeben ist:

1. Die personenbezogenen Daten sollen 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.
2. Die betroffene Person hat in die erneute Verarbeitung eingewilligt.

> **Hinweis:** Hinsichtlich der Einwilligung zur erneuten Verarbeitung gelten die Voraussetzungen der Art. 7 + 8 DSGVO.

9. Wer ist für das Löschen und Einschränken verantwortlich?

Generell trifft das Unternehmen die Verantwortung für die Einhaltung datenschutzrechtlicher Vorgaben. Aber es trifft auch jeden Mitarbeiter eine gewisse Pflicht, auf die Einhaltung datenschutz- rechtlicher Bestimmungen zu achten. Gem. Art. 6 DSGVO dürfen personenbezogene Daten nur unter strengen Voraussetzungen verarbeitet werden. Das Unternehmen (Verantwortlicher) muss gem. Art. 32 Abs. 4 DSGVO sicherstellen, dass die ihm unterstellten Personen personenbezogene Daten nur auf Anweisung und gem. den datenschutzrechtlichen Regelungen verarbeiten. Zur Verarbeitung zählt auch das Speichern und damit das Nichtlöschen.

Impressum

Dies ist ein Ratgeber der TKMmed!a, einem Unternehmensbereich des
VNR Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2-4
53177 Bonn
Großkundenpostleitzahl: D-53095 Bonn

Tel.: 0228 – 9 55 0 150 (Kundendienst)
Fax: 0228 – 3 69 64 80

Ust.-ID: DE 81263972
Amtsgericht Bonn, HRB 8165

Internet: www.tkm-media.de
E-Mail: kundendienst@vnr.de

Bildnachweis: Stockwerk-Fotodesign - Fotolia.com (www.fotolia.com)

Layout & Satz: Elisabeth Whitley, rheinschrift

Vorstand: Richard Rentrop