PRODATIS®

The eBusiness Solution Company.

Das Löschkonzept – ein Beispiel

Um seinen Löschpflichten nachkommen zu können, ist es notwendig, dass der Verantwortliche ein Löschkonzept erstellt, dokumentiert und umsetzt. Dieser Artikel gibt Tipps zum Aufbau eines solchen Konzepts.

Mitten im Block der Betroffenenrechte findet sich in der Datenschutz-Grundverordnung (DSGVO) der Artikel 17 mit seinem „Recht auf Löschung", auch „Recht auf Vergessenwerden" genannt.
Da liegt es nahe, zu denken, dass dies etwas ist, was die betroffene Person aktiv wahrnimmt. Wer so denkt, denkt nicht weit genug.

Das Recht auf Löschung

Schaut man sich Art. 17 DSGVO an, erweckt er zunächst den Eindruck, die betroffene Person müsse selbst von diesem Recht Gebrauch machen („Die betroffene Person hat das Recht … zu verlangen …"). Weiter heißt es: „der Verantwortliche ist verpflichtet", was logischerweise den Gegenpart zu „hat das Recht" darstellt.

Hat jemand einen Rechtsanspruch, muss ihn das entsprechende Gegenüber erfüllen.

Das ist jedoch nur die eine Seite der Medaille. Denn der Verantwortliche kann sich, was das Löschen angeht, nicht darauf zurückziehen, dass er dem Löschgebot nur dann nachkommt, wenn die betroffene Person ihre Ansprüche geltend macht.

Die Auflistung in Art. 17 Abs. 1 DSGVO legt fest, wann der Verantwortliche die Daten unverzüglich zu löschen hat, unabhängig davon, ob die betroffene Person ein Löschen einfordert.

Das gilt etwa, wenn die Zwecke für die Verarbeitung der personenbezogenen Daten entfallen. Das Gleiche gilt bei unrechtmäßiger Verarbeitung. Und noch weitere Gründe finden sich in Art. 17 Abs. 1 Buchst. b, d–f DSGVO.

Zusätzlich zum reaktiven Löschen auf Anforderung durch die betroffene Person muss sich der Verantwortliche also Gedanken zum aktiven, zyklischen Löschen ohne Anforderung durch die betroffene Person machen.

Das geht nicht ohne ein Löschkonzept.

Der Grundsatz der Speicherbegrenzung
Die Löschung personenbezogener Daten nach Art. 17 DSGVO ist ein elementarer Baustein, um den Grundsatz der Speicherbegrenzung zu erfüllen (Art. 5 Abs. 1 Buchst. c und e DSGVO).

Das betont auch noch einmal der Erwägungsgrund 39 Satz 8 DSGVO: „Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt."

Was ist eine Löschung eigentlich?
Unter Löschung versteht man im Allgemeinen das physische, nicht rückgängig zu machende Vernichten von digitalen personenbezogenen Daten auf einem Datenträger bzw. das datenschutzkonforme Vernichten analoger Datenträger wie Papier oder Mikrofiche nach DIN 66399.

Bei digitalen Daten genügt nach Ansicht der österreichischen Datenschutzaufsichtsbehörde eine Anonymisierung der personenbezogenen Daten den Anforderungen aus Art. 17 DSGVO (siehe hierzu https://ogy.de/DSBT-20181205).

Diese Festlegung der österreichischen Aufsichtsbehörde ist ein valides Fundament, das als Rechtfertigung für die Anonymisierung personenbezogener Daten gelten kann, sofern eine physische Löschung für den Verantwortlichen unzumutbar ist.

Valide deswegen, weil sich im Rahmen der von der DSGVO geforderten Kohärenz der Aufsichtsbehörden davon ausgehen lässt, dass andere Aufsichtsbehörden schwerlich widersprechen können.

Herausforderungen für das gesetzeskonforme Löschen
Beim Löschen von personenbezogenen Daten befindet sich der Verantwortliche in einem kritischen Spannungsfeld – und das sowohl beim reaktiven als auch beim aktiven, zyklischen Löschen.

Dem Recht auf unverzügliche Löschung gemäß Art. 17 DSGVO auf der einen Seite steht auf der anderen Seite eine Vielzahl gesetzlicher Aufbewahrungsfristen gegenüber. Sie verbieten, sofern sie zutreffen, ein Löschen, zumindest für eine bestimmte Zeit.

So stehen der unverzüglichen Löschung möglicherweise steuerrechtliche Aufbewahrungspflichten bei Kaufverträgen entgegen, wie sie sich beispielsweise im Steuerrecht (vgl. § 147 Abgabenordnung (AO)) finden.

Gesetzliche Aufbewahrungspflichten
Art. 6 Abs. 1 Buchst. c DSGVO erlaubt die Verarbeitung, wenn sie „zur Erfüllung einer rechtlichen Verpflichtung erforderlich" ist, „der der Verantwortliche unterliegt". Eine solche Verpflichtung liegt im beschriebenen Fall vor, sodass das vorrangige Recht, hier § 147 AO, anzuwenden ist.

Der Verantwortliche darf den Datensatz demnach selbst dann nicht vor Ablauf der Aufbewahrungsfrist löschen, wenn die betroffene Person die Löschung einfordert oder der Zweck der Verarbeitung entfallen ist.

Weitere Quellen von verbindlichen Aufbewahrungsfristen können Handelsgesetzbuch (HGB), Geldwäschegesetz (GwG), Wertpapierhandelsgesetz (WpHG) u.a. sein.

Weitere Ausnahmen
Darüber hinaus liefert Art. 17 Abs. 3 DSGVO Ausnahmen, die einer unverzüglichen Löschung entgegenstehen. So heißt es u.a. in Art. 17 Abs. 3 Buchst. c DSGVO: „Soweit die Verarbeitung erforderlich ist … zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen."

Ein Beispiel hierfür ist der Bewerbungsprozess. Der Verantwortliche verarbeitet die personenbezogenen Daten des Bewerbers nach Art. 6 Abs. 1 Buchst. b („vorvertragliche Maßnahmen").

Sagt er dem Bewerber ab, weil dieser nicht der Gesuchte ist, entfällt zunächst vordergründig die Rechtsgrundlage zur Verarbeitung, weil der Zweck entfällt.

Hier greift nun die Ausnahme nach Art. 17 Abs. 3 Buchst. c DSGVO. Der Verantwortliche benötigt die Daten weiterhin, um mögliche Rechtsansprüche resultierend aus dem

Allgemeinen Gleichbehandlungsgesetz (AGG) abwehren zu können.

Dort heißt es in § 15 Abs. 4 AGG: „Ein Anspruch … muss innerhalb einer Frist von zwei Monaten schriftlich geltend gemacht werden … Die Frist beginnt im Falle einer Bewerbung … mit dem Zugang der Ablehnung …“

Somit ist eine fortdauernde Verarbeitung (hier Speicherung oder Aufbewahrung) bis zum Ende der Einspruchsfrist erlaubt, und der Verantwortliche muss die Daten erst nach Ablauf dieser Frist unverzüglich löschen.

So erstellen Sie die Löschmatrix

Das Löschkonzept soll sicherstellen, dass der Spagat zwischen „Löschen müssen“ und „nicht Löschen dürfen“ für alle personenbezogenen Daten im Unternehmen gelingt.

Die hierin festgelegten Regelungen gelten sowohl für das aktive als auch für das reaktive, zyklische Löschen.

Ebene 1: Gruppen von betroffenen Personen

Um Ihre Löschregeln zu definieren, beginnen Sie damit, Ihre personenbezogenen Daten zu kategorisieren. Diese Informationen sollten sich im Verzeichnis von Verarbeitungstätigkeiten finden. Wenn nicht, fragen Sie sie in allen Abteilungen, die personenbezogene Daten verarbeiten, ab. (Und weisen Sie den Verantwortlichen darauf hin, das Verzeichnis schnellstmöglich zu ergänzen.)

Bilden Sie hierbei zunächst ein übergeordnetes Cluster verschiedener Arten betroffener Personen. Diese erste Ebene ermöglicht es Ihnen insbesondere beim reaktiven Löschen, die Fristen schneller zuzuordnen.

Sind alle Verarbeitungstätigkeiten analysiert, werden Sie wahrscheinlich eine Liste von Gruppen betroffener Personen wie die folgende erhalten.

Diese Gruppen bilden die erste Ebene Ihrer Löschmatrix:

- Mitarbeiter
- Kunden
- Lieferanten
- Besucher
- Patienten

Die Liste, die die betroffenen Personen auf erster Ebene in Gruppen einteilt, kann in Ihrem Unternehmen durchaus abweichend sein, sofern Sie personenbezogene Daten von weiteren oder von weniger Gruppen verarbeiten.

Ebene 2: Datenkategorien erstellen

Als zweite Ebene fassen Sie innerhalb jeder Gruppe nun die unterschiedlichen „Datenkategorien“ sinnvoll zusammen.

Am Beispiel von Mitarbeiterdaten sei dies im Folgenden exemplarisch durchgespielt.

„Sinnvoll“ bedeutet, artverwandte Daten wie z.B. Name, Geburtsdatum und Geschlecht einem Personenstammsatz zuzuordnen, während die Kontaktdaten und der Familienstand bei den ergänzenden Informationen zusammengefasst werden.

Der Vorteil, die Datenkategorien in einem Cluster zusammenzufassen, liegt darin, dass Sie ähnliche Datenarten gleich behandeln und Datenarten, die bei einer neuen Verarbeitungstätigkeit neu auftreten, den vorhandenen Gruppen zuordnen können.

So lassen sich für die Gruppe „Mitarbeiter“ z.B. folgende Datenkategorien festlegen:

<u>Mitarbeiter</u>

- Personenstammsatz
- ergänzende Informationen
- Postanschriften
- Artikel-9-Daten (besondere Kategorien personenbezogener Daten)
- Berechtigungen
- Bewerbungsunterlagen
- Bankdaten
- Vorsorgeleistungen des Arbeitgebers
- Steuerinformationen
- Reisekosten

- Ausweispapiere
- Log-Daten
- Profildaten

Alle personenbezogenen Daten eines Mitarbeiters werden nun diesen Datenkategorien zugeordnet.

So würden etwa die Telefonnummer, die E-Mail-Adresse, die Nationalität und Sprachkenntnisse den „ergänzenden Informationen", die Dienst- und die private Anschrift hingegen den „Postanschriften" zugeordnet.

Informationen zur Schwerbehinderung oder zu Arbeitsunfähigkeiten gehören zur Kategorie der „Artikel-9- Daten".

Ebene 3: Status der Gruppe von betroffenen Personen
Die dritte Ebene definiert den „Status der Gruppe von betroffenen Personen". Bei der Gruppe „Mitarbeiter" bieten sich folgende drei Status an, die exemplarisch am Personenstammsatz dargestellt seien:

Mitarbeiter
- Personenstammsatz
  - Bewerber
  - aktiver Mitarbeiter
  - ausgeschiedener Mitarbeiter

Ist die Gruppe von betroffenen Personen „Kunde", stünde in der dritten Ebene beispielsweise „Interessent", „Akquisition", „aktiver Kunde" und „abgewickelter Kunde".

Ebene 4: Status des Datensatzes
Als vierte Ebene kommt nun noch die Qualität der verarbeiteten Daten hinzu. Diese Ebene bezeichnen wir als „Status des Datensatzes". Verständlicherweise sind aktuelle Daten anders zu behandeln als veraltete, sodass diese Ebene zwei Status enthält.

In der Matrix sieht es dann am Beispiel „aktiver Mitarbeiter" wie folgt aus:

Mitarbeiter
- Personenstammsatz
  - aktiver Mitarbeiter
    - aktuell
    - veraltet

Diese Auswahl ist für alle Kombinationen der Ebenen 1 bis 3 identisch.

Die Kombinationen der Ebenen 3 und 4 bilden den Lebenszyklus des Datensatzes ab – also von der Wiege bis zur Bahre.

Der Mitarbeiter beginnt als „Bewerber" und wird über „aktiver Mitarbeiter" bis hin zum ausgeschiedenen Mitarbeiter in der Verarbeitung geführt.

Seine Daten sind dabei entweder aktuell oder veraltet.

Die Löschfrist beginnt immer am Ende des Lebenszyklus, der Datensatz wird quasi „beerdigt".

Die Matrix steht – nun noch Löschfristen hinzufügen
Haben Sie alle Kombinationen der Ebenen 1 bis 4 erstellt, erhalten Sie schnell eine Löschmatrix mit 250 und mehr Zeilen.

Im nächsten Schritt geht es nun darum, die Verarbeitungs- und Aufbewahrungsfristen zuzuordnen. Die Verarbeitungsfristen orientieren sich dabei am Zweck und der Notwendigkeit der Datenverarbeitung. Sie definieren den spätesten Zeitpunkt der Löschung.

Die Aufbewahrungsfristen hingegen bilden die gesetzlichen Fristen ab und bestimmen den frühesten Zeitpunkt der Löschung.

Daraus ergeben sich mindestens zwei Verarbeitungszustände: Verarbeitung und Löschung.

Gegebenenfalls kann ein dritter Zustand, Sperrung, hinzukommen. In diesem Zustand ist der Zugriff auf die personenbezogenen Daten stark limitiert oder gar unterbunden.

Die entsprechenden Verarbeitungszustände sind in der fol-

genden Grafik farblich dargestellt. Grün bedeutet „Verarbeitung", gelb „zu sperren/gesperrt" und rot „zu löschen".

Die festzulegenden Zeitpunkte lassen sich ebenfalls in Clustern abbilden, um eine Standardisierung innerhalb der Löschmatrix zu erhalten.

So sind z.B. folgende Stufen denkbar, die sich an verschiedenen gesetzlichen Aufbewahrungsfristen orientieren:

- sofortige Löschung
- nach 1 Monat
- nach 6 Monaten
- nach 1 Jahr
- nach 3 Jahren
- nach 6 Jahren
- nach 10 Jahren
- nach 30 Jahren

Trotz der vielen Informationen ergibt sich daraus eine recht übersichtliche Löschmatrix:
ACHTUNG: Im Kontext von international agierenden Konzernen ist bei der Zuordnung der Löschfristen zu berücksichtigen, dass es durchaus unterschiedliche Aufbewahrungsfristen in den einzelnen Ländern gibt.

Fertig?
Nicht ganz. Zu guter Letzt heißt es „nur" noch, diese Löschmatrix in allen IT-Systemen zu implementieren.

Das bedeutet, Routinen zum zyklischen Löschen zu aktivieren, die die Datensätze anhand ihres Status (Ebene 1–4) erkennen und entsprechend der Löschmatrix unangetastet lassen, sie sperren oder bei Notwendigkeit löschen.

Ein absolut nicht einfaches Unterfangen, da manche IT-Systeme das physische Löschen nicht zulassen. Eine Alternative ist, die Daten zu anonymisieren.

Jetzt fertig? Nein, leider nicht, denn auch digitale personenbezogene Daten in unstrukturierten IT-Systemen unterliegen den Anforderungen der DSGVO und sind demnach zyklisch zu löschen.

Hierzu gehören z.B. Office-Dokumente auf Fileshares oder lokalen Festplatten. Ihre regelmäßige Löschung lässt sich nahezu ausschließlich organisatorisch über entsprechende Prozesse und Anweisungen abbilden. Das Gleiche gilt übrigens für analoge Daten wie Papierdokumente oder Mikrofiches.

Löschmatrix für den Personenstammsatz der Gruppe „Mitarbeiter"

Gruppe betroffener Personen	Datenkategorie	Status der Gruppe der betroffenen Personen	Status des Datensatzes	Sofort	nach 1 Monat	nach 6 Monaten	nach 1 Jahr	nach 3 Jahren	nach 6 Jahren	nach 10 Jahren	nach 30 Jahren
Mitarbeiter	Personenstammsatz	Bewerber	aktuell								
			veraltet								
		aktiver Mitarbeiter	aktuell								
			veraltet								
		ausgeschiedener Mitarbeiter	aktuell								
			veraltet								
	ergänzende Informationen										
Ebene 1	Ebene 2	Ebene 3	Ebene 4	Löschfristen							

Verarbeitung
zu sperren/gesperrt
zu löschen

Erst wenn auch hier alle Maßnahmen umgesetzt und dokumentiert sind, ist das Löschkonzept vollständig.

In aller Kürze
Fassen Sie alle personenbezogenen Daten in sinnvolle Cluster zusammen. Grundlage für die Cluster auf erster Ebene ist zunächst die Art der betroffenen Personen.

Erstellen Sie innerhalb der Cluster der ersten Ebene erneut Cluster, dieses Mal auf Basis der Datentypen.

Zwei weitere Ebenen bilden den Lebenszyklus der Daten während der Verarbeitung ab. Weisen Sie den Kombinationen der vier Ebenen jeweils Mindestaufbewahrungsfristen und Maximalverarbeitungszeiten zu.

So entsteht eine übersichtliche Löschmatrix, anhand derer sich ein Löschkonzept umsetzen lässt.

Quelle:
www.datenschutz-praxis.de