DSGVO-konformes Datenlöschen bedeutet Löschkonzepte erstellen, vorhalten und zur Anwendung bringen

Beispiel:

Satte 14,5 Millionen Euro Strafe für ein System, in dem keine personenbezogenen Daten gelöscht werden konnten, traf Ende 2019 die ‚Deutsche Wohnen SE'. Die Datenschutzaufsichtsbehörde hatte bei einer Prüfung festgestellt, dass das Unternehmen personenbezogene Daten von Mietern in einem Archivsystem speicherte, dort aber keine Möglichkeit implementiert war, die Daten wieder zu löschen. Bislang wurde die Zahlung wegen eines Verfahrenshindernisses durch die 26. Große Strafkammer des Landgerichts Berlin abschlägig beschieden, da ein Bußgeldverfahren nur gegen eine natürliche, nicht aber gegen eine juristische Person geführt werden kann. Sprich eine Ordnungswidrigkeit kann per se nur durch natürliche Person begangen worden sein, wobei die Datenschutzaufsichtsbehörde eben gerade keine natürliche Person für den durchaus gravierenden Datenschutzverstoß / -mangel benannt hatte. Abgesehen von der Tatsache, dass hier wohl noch „nachgebessert" werden könnte, war der Imageschaden auf jeden Fall gravierend.

https://www.heise.de/news/Gravierende-Maengel-Deutsche-Wohnen-wendet-DSGVO-Millionenstrafe-vorerst-ab-5064633.html

Was man am vorhergehenden Beispiel gut erkennen kann: es ist nicht nur wichtig die Erfassungslage zu klären, sondern auch Fristen und geeignete Maßnahmen abzubilden, wie, wann und durch wen die erfassten Daten gelöscht werden. Und damit ist man beim Thema „Löschkonzepte“.

Was ist ein Löschkonzept?

Kurz gefasst die Festlegung, wie und wann personenbezogene Daten gelöscht werden, wenn sie das Ende ihres Lebenszyklus erreicht haben. Was mit Blick auf die EU-DSGVO spätestens dann eintritt, wenn der Erhebungszweck abgelaufen ist. Ein Löschkonzept ist also die schriftlich erfasste und somit fixierte Form, die dem ganzen Prozedere einen systematischen Rahmen gibt.

Braucht man Löschkonzepte?

Aus rechtlicher Sicht und somit im Einklang mit Art. 30 EU-DSGVO sollte das obligatorische Verzeichnis von Verarbeitungstätigkeiten Löschfristen für Datenkategorien ausweisen. Daneben ist es - je nach Unternehmensgröße - schwierig den Überblick ohne Löschkonzepte zu behalten, wodurch auch ein ganz praktischer Grund vorliegt.

Grundlegende Fragen zu Löschkonzepten

- ⇨ Welche Löschregeln gelten für welche Daten?
- ⇨ Wie erfolgt die Implementierung der Löschregeln?
- ⇨ Wie und durch wen erfolgen die Dokumentierung und Verifizierung von Löschregeln, Implementierungsspezifikationen und den konkreten Löschmaßnahmen?
- ⇨ Welche Person oder Stelle ist für die Aufgaben, die aus dem Löschkonzept entstehen, verantwortlich? Wie und durch wen erfolgt die Aktualisierung und Weiterentwicklung?

Erste Schritte

- ⇨ Identifikation der Stellen, an denen personenbezogene Daten erhoben werden.

- ⇨ Kategorisierung dieser Daten.

- ⇨ Definierung von Löschregeln für die aufgestellten Kategorien.

Die DIN-Norm 66398 kann hierbei als Hilfe herangezogen werden, da sie quasi Leitlinien an die Hand gibt: https://din-66398.de/

Löschfristen, Löschklassen, Löschregeln
– ein kompaktes, praktisches Instrumentarium

Löschfristen geben die Aufbewahrungszeit und somit auch den Löschtermin vor. Hier können auch gesetzliche Vorgaben (Aufbewahrungsfristen) eine Rolle spielen. Ansonsten empfehlen sich Standard-Löschfristen zu definieren.

Eine **Löschklasse** fasst alle Daten, die mit dem gleichen Verarbeitungszweck, dem gleichen Startzeitpunkt und den gleichen Löschfristen zusammen. So ergeben sich in der Regel eine überschaubare Anzahl von Löschklassen.

Jeder Löschklasse wird im Anschluss eine **Löschregel** zugewiesen.

Tipp: Über jede Anwendung eines Löschkonzeptes sollte Protokoll geführt werden. Und es schadet auch nicht, dass nach Hinweis auf bestehende Löschkonzepte, die zuständigen Personen / Stellen diesen Informationserhalt quasi „quittieren“.

-Anhang-

Betrachtungsgrundlage EU-DSGVO, Art. 17: Recht auf Löschung ("Recht auf Vergessenwerden")

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten

angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Kapitel IV - Verantwortlicher und Auftragsverarbeiter

Abschnitt 1 - Allgemeine Pflichten

Artikel 30 Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

- die Zwecke der Verarbeitung;

- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

#ph