Löschkonzepte und deren Umsetzung

Das Löschen personenbezogener Daten erfordert planvolles Vorgehen. Schließlich sollen die richtigen Daten zur richtigen Zeit am richtigen Ort gelöscht werden.

Ein Whitepaper von Stefan Hessel, LL.M. und Christina Kiefer, LL.M.

Risiken ohne datenschutzkonformes Löschen

Das regelmäßige Löschen personenbezogener Daten gehört zu den Grundlagen der datenschutzrechtlichen Compliance. Gerade für Unternehmen mit einem großen Datenbestand und einer über die Jahre gewachsenen IT-Infrastruktur ist datenschutzkonformes Löschen eine erhebliche Herausforderung. Es ist nicht damit getan, personenbezogene Daten auf Anfrage des Betroffenen zu löschen. Die Datenschutz-Grundverordnung (DSGVO) erfordert eine Speicherbegrenzung und damit ein regelmäßiges Löschen. Wird nicht gelöscht, drohen empfindliche Bußgelder oder Schadensersatzansprüche. Außerdem gefährden löschungsreife Altdaten die Datenqualität und werden somit zu einem Hemmschuh der datengetriebenen Digitalisierung eines Unternehmens. Je größer der Datenbestand, desto größer das Risiko, dass Datenschutzverletzungen oder IT-Sicherheitsvorfälle zu Bußgeldern und/oder Schadensersatzforderungen führen.

Das Löschkonzept

Um den Verpflichtungen aus der DSGVO ordnungsgemäß nachkommen zu können, benötigen Unternehmen ein Löschkonzept. Dies folgt daraus, dass die DSGVO den Grundsatz der Speicherbegrenzung und der Rechenschaftspflicht festlegt. Nach der DSGVO darf der Verantwortliche personenbezogene Daten nur in einer Form speichern, die die Identifizierung der betroffenen Personen so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Der Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO besagt, dass der Verantwortliche die Einhaltung der Grundsätze nachweisen muss. Es ist anerkannt, dass dies durch das Erstellen eines Löschkonzepts möglich ist.[1] In Fällen, in denen Unternehmen kein Löschkonzept vorweisen konnten, haben die Datenschutzaufsichtsbehörden verschiedener europäischer Länder in der Vergangenheit bereits Bußgelder verhängt.[2]

Es existieren diverse Muster, an denen man sich bei der Erstellung eines entsprechenden Konzepts orientieren kann. Etwa die DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten", die sich zwar noch auf die Rechtslage unter dem Bundesdatenschutzgesetz (BDSG) bezieht, aber praktisch bewährt und auf die aktuelle Rechtslage übertragbar ist.[3] Solche schematischen Vorgaben können

---

[1] *Voigt*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 5 DS-GVO Rn. 34.
[2] Statt aller: Newsmeldung: Danish SA: fine proposed for Danske Bank, abrufbar unter: https://edpb.europa.eu/news/national-news/2022/danish-sa-fine-proposed-danske-bank_de, zuletzt abgerufen: 03.04.2023
[3] *Voigt*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 5 DS-GVO Rn. 35.

jedoch nur Ausgangspunkt für die Entwicklung eines Löschkonzepts sein. Es gilt, der Individualität des betroffenen Unternehmens Rechnung zu tragen.

Das Ziel eines Löschkonzepts ist es, durch klare Festlegungen einen geordneten Prozessablauf zu gewährleisten, damit im Zeitpunkt der Löschung keine wichtigen Aspekte übersehen werden.[4] Vorteile bestehen auch darin, dass ein klares Löschkonzept Datenschutzverantwortliche im Unternehmen entlastet, da diese in den Standardfällen nicht mehr konsultiert werden müssen.[5]

Das Löschkonzept sollte nicht isoliert neben anderen Prozessen stehen. Idealerweise sollte es sowohl mit dem Löschen als Reaktion auf etwaige Löschanträge nach Art. 17 Abs. 1 DSGVO als auch mit einem Berechtigungs- und Rollenkonzept abgestimmt werden.[6]

Was muss gelöscht werden?

Der erste Schritt bei der Erarbeitung eines Löschkonzepts ist die Identifikation der personenbezogenen Daten, die im Unternehmen verarbeitet werden. Verschiedene Datenarten können anhand des Zwecks der Datenverarbeitung differenziert und bestimmten Datenobjekten zugeordnet werden. Ein Beispiel für eine Datenart wären etwa Buchhaltungsdaten, denen als Datenobjekte Buchungssätze und Rechnungen sowie Zahlungstransaktionen mit Banken zugeordnet sind.[7]

Löschfristen

Sind die personenbezogenen Daten identifiziert, müssen die Löschfristen ermittelt werden. Würde man den Zweckbindungsgrundsatz streng anwenden, wären personenbezogene Daten unmittelbar im Augenblick des Zweckfortfalls zu löschen. Dies würde Unternehmen, die große Datenbestände verwalten, vor eine unlösbare Aufgabe stellen. Erwägungsgrund Nr. 39 zur DSGVO besagt, dass der Verantwortliche Fristen für die Löschung von personenbezogenen Daten oder regelmäßige Überprüfung vorsehen sollte. Daraus ergibt sich, dass ein gewisses Maß an Schematisierung in Form einer regelmäßigen Überprüfung ausreichend sein kann. Die Löschfristen hängen nicht zuletzt von der Sensibilität der betroffenen Daten ab. Idealerweise ergibt sich aus dem Löschkonzept für jede Datenart eindeutig, wann Daten von dieser Art zu löschen sind, damit Mitarbeiter ohne weitere Rückfragen der Löschverpflichtung nachkommen können.[8]

Aufbewahrungspflichten

Das Recht kennt nicht nur Lösch-, sondern auch Aufbewahrungspflichten, die in einem Löschkonzept zwingend zu berücksichtigen sind, um nicht durch eine datenschutzrechtliche Übererfüllung gegen andere Rechtsvorschriften zu verstoßen.

Eine im Wirtschaftsverkehr bedeutende Vorschrift stellt § 257 Handelsgesetzbuch (HGB) dar. Danach ist jeder Kaufmann verpflichtet, bestimmte Unterlagen, wozu Handelsbücher, Handelsbriefe oder Belege für Buchungen zählen, je nach Kategorie sechs oder zehn Jahre aufzubewahren. Darüber hinaus ergeben sich Aufbewahrungspflichten aus dem Steuerrecht. § 147 Abgabenordnung (AO) ordnet in Abs. 1 Nr. 3 unter anderem an, dass neben

---

[4] *Wehrmann*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, Löschkonzept, Anm. 1-8.
[5] Ebd., Anm. 7.
[6] Ebd., Anm. 1.
[7] *Conrad,* in: Auers-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 34 Recht des Datenschutzes, Rn. 623 f.
[8] *Voigt*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 5 DS-GVO Rn. 36.

Handels- auch Geschäftsbriefe aufbewahrt werden müssen.

Daneben existieren Aufbewahrungsrechte, die nicht verpflichtend sind, aber einem anerkannten rechtlichen Interesse des Verantwortlichen dienen. Nach Art. 17 Abs. 3 lit. e DSGVO entfällt die Pflicht zum Löschen der Daten, wenn diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dienen. Dies ist jedenfalls dann der Fall, wenn Auseinandersetzungen anstehen oder mit hinreichender Wahrscheinlichkeit zu erwarten sind.[9] Daraus ergeben sich große Unsicherheiten. Es dürfte in der Praxis oft schwierig sein, nach objektivierbaren Kriterien zu bestimmen, ob eine Auseinandersetzung hinreichend wahrscheinlich ist. Gleichzeitig ist es in vielen Fällen, etwa innerhalb der Frist, in der Kunden Gewährleistungsrechte geltend machen können, unverzichtbar, bestimmte Daten weiter zu speichern. Um datenschutzrechtliche Risiken zu minimieren und notwendige Daten, die im Interesse des Unternehmens liegen, nach Möglichkeit zu speichern, bedarf es einer rechtlichen Bewertung der infrage stehenden Daten im Einzelfall.

Anonymisieren statt Löschen?

Bei der Erfüllung von Löschfristen stellt sich unvermeidbar die Frage, welche Anforderungen die DSGVO an den Vorgang des Löschens selbst stellt. Die DSGVO gibt anders als bei zahlreichen Begriffen der Verordnung keine ausdrückliche Definition vor. Unter dem Löschen personenbezogener Daten ist das Unkenntlichmachen dieser Daten zu verstehen.[10] Durch das Löschen muss es unmöglich gemacht werden, dass die in den Daten enthaltenen personenbezogenen Informationen mit verhältnismäßigem Aufwand zur Kenntnis genommen werden können.[11] Daraus folgt zum Beispiel, dass die bloße Betätigung der Löschentaste keine ausreichende Löschung im datenschutzrechtlichen Sinne darstellt.

Es ist fraglich, ob darüber hinaus nicht Möglichkeiten bestehen, wie Unternehmen ihren Löschpflichten nachkommen und trotzdem weiter wirtschaftlich von den Daten profitieren können. Die DSGVO findet nur auf personenbezogene Daten Anwendung. Daher ist es denkbar, die Verpflichtung durch Aufhebung des Personenbezugs des Datums, d.h. durch Anonymisierung, zu erfüllen. Dies kann für ein Unternehmen interessant sein, um ggf. statistische oder sonstige Informationen zu behalten, die für Big Data oder Anwendungen der künstlichen Intelligenz (KI) auch nach Aufhebung des Personenbezuges von Nutzen sein können. Soweit ersichtlich, ist die Frage, ob die Löschverpflichtung auch durch das Anonymisieren von Daten erfüllt werden kann, noch nicht durch die Rechtsprechung entschieden worden. Es sprechen jedoch gute Gründe dafür, eine Anonymisierung ausreichen zu lassen – eine Auffassung, der auch der Bundesdatenschutzbeauftrage zuzuneigen scheint.[12]

Es ist jedoch zu beachten, dass die entsprechenden Daten tatsächlich so bearbeitet werden müssen, dass kein Bezug zu der betroffenen Person mehr hergestellt werden kann. Es bedarf daher einer genauen Prüfung, ob im Unternehmen weitere Daten vorhanden sind, aus denen sich in einer

---

[9] *Meents/Hinzpeter*, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, Art. 17 DS-GVO Rn. 133.
[10] *Arning/Rothkegel*, in: Taeger/Gabel, DS-GVO - BDSG - TTDSG, Art. 4 DS-GVO Rn. 98.
[11] Ebd.
[12] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 8 f., abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung, zuletzt abgerufen: 03.04.2023.

Zusammenschau doch noch eine Identifizierbarkeit der Person ergibt. Zumindest ob dies auch für das Erfüllen der Löschverpflichtung nach Art. 17 DSGVO auf Antrag des Betroffenen gilt, ist dies allerdings umstritten.[13] Unternehmen sollten entsprechende Entwicklungen in dieser Frage beobachten, um die etwaigen Möglichkeiten, Daten in anonymisierter Form gewinnbringend weiterzuverwenden, tatsächlich auszuschöpfen.

Was droht bei Verstößen?

Wie real die Gefahr negativer Konsequenzen bei fehlenden oder mangelhaften Löschkonzepten ist, verdeutlichen zahlreiche Bußgeldbescheide europäischer Datenschutzaufsichtsbehörden der letzten Jahre. Die *Commission Nationale de l'Informatique et des Libertés (CNIL)* hat etwa bei dem französischen Staatsbetrieb *RATP* zahlreiche Verstöße gegen die DSGVO festgestellt und, nicht zuletzt wegen der Verarbeitung von Daten über den für den Zweck erforderlichen Zeitraum hinaus, ein Bußgeld in Höhe von 400.000 Euro verhängt.[14]

Auch in Deutschland drohen erhebliche Konsequenzen. Zurzeit ist beim Kammergericht in Berlin ein Verfahren rechtshängig, in dem es um ein Bußgeld in Höhe von 14,5 Millionen Euro geht, das die Berliner Datenschutzaufsichtsbehörde im September 2019 gegen den Immobilienkonzern *Deutsche Wohnen* verhängte. Vorgeworfen wird dem Konzern, nicht mehr erforderliche Daten früherer Mieter in einem Archivsystem gespeichert zu haben, in dem diese nicht mehr gelöscht werden konnten. Zwar ist der Ausgang des Verfahrens noch unklar, es verdeutlicht jedoch, dass fehlende Löschkonzepte zu erheblichen finanziellen Konsequenzen führen können.[15] Unternehmen sollten solche Risiken nach Möglichkeit ausräumen.

Daneben drohen etwa beim verspäteten Löschen nach einem Antrag gemäß Art. 17 DSGVO oder der unrechtmäßigen Verarbeitung von personenbezogenen Daten nach Wegfall des Zwecks Schadensersatzansprüche nach Art. 82 DSGVO durch den Betroffenen. Unsere Auswertung der aktuellen Rechtsprechung zu Art. 82 DSGVO zeigt, dass insbesondere in der Arbeitsgerichtsbarkeit den Betroffenen ein Schadensersatz zugesprochen wird.[16] Die Höhe des von den Gerichten zugesprochenen Schadensersatzes liegt durchschnittlich im vierstelligen Bereich.[17] Um solche Risiken zu minimieren, sollte das datenschutzkonforme Löschen Teil der Datenschutz-Compliance jedes Unternehmens sein.

Schritte zum datenschutzkonformen Löschen

Das datenschutzkonforme Löschen von personenbezogenen Daten im Unternehmen bedarf einer sorgfältigen Analyse und Planung. Kern der Datenlöschung ist das

---

[13] *Roßnagel*, ZD 2021, 188, 192.
[14] Newsmeldung: Französische Datenschutzaufsicht verhängt Bußgeld in Höhe von 400.000 Euro, abrufbar unter: https://www.reuschlaw.de/news/franzoesische-datenschutzaufsicht-verhaengt-bussgeld-in-hoehe-von-400-000-euro/, zuletzt abgerufen: 03.04.2023.
[15] Newsmeldung: Datenschutzbußgeldverfahren gegen die „Deutsche Wohnen" vor dem EuGH, abrufbar unter: https://www.behoerden-spiegel.de/2023/01/20/datenschutzbussgeld-verfahren-gegen-die-deutsche-wohnen-vor-dem-eugh/, zuletzt abgerufen: 03.04.2023.
[16] reuschlaw Report: Risiko bei Schadensersatzklagen wegen Datenschutzverstößen, abrufbar unter: https://www.reuschlaw.de/news/reuschlaw-report-risiko-bei-schadensersatzklagen-wegen-datenschutzverstoessen/, zuletzt abgerufen: 03.04.2023.
[17] Ebd.

Löschkonzept, das als Handbuch des Löschens im Unternehmen sämtliche wichtigen Punkte zur Löschung von personenbezogenen Daten als Richtschnur vorgibt. Rechtliche Anforderungen an das Löschen, die Identifizierung der relevanten Aufbewahrungsrechte und Aufbewahrungspflichten, Anforderungen an das datenschutzkonforme Löschen sowie die Prozesse zum Löschen einschließlich eines Rollen- und Berechtigungskonzepts für Löschentscheidungen werden hier abgebildet. Ein Löschkonzept umfasst typischerweise strukturierte und unstrukturierte Daten sowie analoge Daten und Datenträger. Einen zentralen Baustein bei der Erstellung des Löschkonzepts stellen die Parameter für die Bestimmung der jeweiligen Löschfristen dar. Dabei sind Aspekte wie die Sensibilität der betroffenen Daten und die oben genannten Aufbewahrungspflichten zu berücksichtigen. Teilweise verlangt die Rechtsprechung, wie eine Entscheidung des Oberlandesgerichts (OLG) Dresden zeigt,[18] nicht das gesamte Dokument oder die gesamte Datei, sondern das konkrete Datum der Beurteilung zugrunde zu legen.

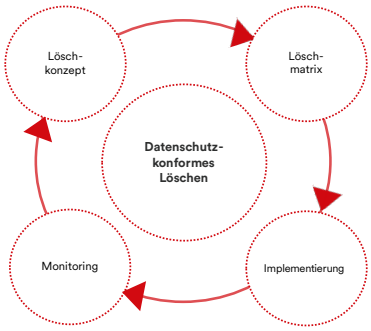

Abbildung 1: Datenschutzkonformes Löschen
© reuschlaw, 2023

Konkretisiert wird das Löschkonzept mithilfe einer Löschmatrix, die in unterschiedlicher Granularität erstellt werden kann. In dieser sind Datenarten Löschklassen zugeordnet und mit den jeweiligen Aufbewahrungs- und Löschfristen sowie den entsprechenden Startzeitpunkten zu versehen.

Umfassende Unterstützung

Wir bieten Ihnen eine vollumfängliche und lückenlose datenschutzrechtliche Beratung bei der Erstellung und Umsetzung von Löschkonzepten. Hierbei unterstützen wir Sie gerne insbesondere mit den folgenden Maßnahmen:

- Erstellung eines Löschkonzepts, das alle relevanten Löschfristen, Aufbewahrungsrechte und -pflichten sowie Festlegung von Rollen und Verantwortlichkeiten und geeignete Löschverfahren enthält;
- Konkretisierung des Konzeptes in einer Löschmatrix;
- Einbeziehung der Abhängigkeiten der gesamten IT-Infrastruktur (inklusive Data- und Dataflow Mappings);
- Internationalisierung Ihres Löschkonzeptes.

Next Step: Kontaktaufnahme

Wir unterstützen Sie gerne bei der Erstellung und konkreten Umsetzung Ihres datenschutzkonformen Löschkonzepts. Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch. Nehmen Sie jetzt unverbindlich Kontakt auf!

T + 49 681 / 859 160 0

E info@reuschlaw.de

[18] OLG Dresden, Urteil vom 14.12.2021, Az. 4 U 1278/21, Rn. 13, abrufbar unter: https://rewis.io/s/u/ZusS/, zuletzt abgerufen: 03.04.2023.