LÖSCHKONZEPT

Johannes Warter

Dr., stellvertretender Programmleiter und rechtlicher Verantwortlicher für das Datenschutzprojekt, Porsche Holding GmbH
Louise-Piëch-Straße 2, 5020 Salzburg, AT
johannes.warter@porsche.co.at

Schlagworte: ***Löschen, Löschkonzept, Sperren***

Abstract: *Personenbezogene Daten werden in Unternehmen in vielen und teils komplexen Systemen und Geschäftsprozessen verarbeitet. Durch rechtliche aber auch interne Vorgaben sind Verantwortliche zur Löschung personenbezogener Daten verpflichtet. Aufgrund der Komplexität ist aber nur ein koordinierter, ganzheitlicher und systematischer Ansatz zur Löschung erfolgsversprechend.*

1. Einleitung

Beim Thema Löschen handelt es sich wohl um den **schwierigsten und komplexesten Teil** der Umsetzung der DSGVO,[1] der in der Praxis erfahrungsgemäß den größten Aufwand bei der Implementierung der rechtlichen Bestimmungen darstellt. Nachfolgend wird eine **praxisbewährte Vorgehensweise** vorgestellt, wie eine Löschlogik für bestehende IT-Systeme gefunden und implementiert werden kann (abstraktes Löschkonzept).

2. Reguläres Löschen – Lebenszyklus von personenbezogenen Daten[2]

Als erster Schritt zur Findung eines koordinierten Löschvorgehens sind Regellöschfristen für sämtliche Datenverarbeitungen zu finden. Dies ist gerade in größeren Unternehmen oft sehr schwierig, da gleiche Daten für verschiedene Zwecke in verschiedenen IT-Systemen verarbeitet werden. Ziel des ersten Schrittes und damit die Grundlage eines koordinierten Löschvorgehens ist die sogenannte **Datenverarbeitungsprozess-/Systeme-Matrix**, welche dem Verantwortlichen eine Zuordnung der verwendeten IT-Systeme einzelner Datenverarbeitungen ermöglicht.

2.1. Identifizieren von personenbezogenen Daten

Zunächst sind personenbezogene Daten zu identifizieren. Werden keine personenbezogenen Daten verarbeitet, sind datenschutzrechtliche Bestimmungen nicht anwendbar.

2.2. Identifizieren aller Datenverarbeitungen

Daraufhin ist es unerlässlich die verschiedenen **(granularen) Datenverarbeitungen**[3] samt der Zwecke zu identifizieren. Die Datenverarbeitungen sollten dabei mit einem eindeutigen Namen versehen werden, damit sie von allen Beteiligten dem Kontext zugeordnet werden können.

---

1 Verordnung (EU) 2016/679, nachfolgend kurz DSGVO.

2 Dieses Vorgehen basiert auf Artikeln von Hammer und eigenen Praxiserfahrungen. Diese werden im Nachfolgenden nicht einzeln zitiert. Siehe näher Hammer/Schuler, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten (2015); Fraenkel/Hammer, Erfahrungen bei der Umsetzung eines Löschkonzeptes, DANA 01/2013, S. 8; Hammer/Schuler, Löschen nach Regeln – die neue Norm hilft, CuA 01/2016, S. 30; Hammer, DIN 66398, DuD 08/2016, S. 528.

3 Zwar ändert sich die Definition der Datenverarbeitung in der DSGVO im Vergleich zum DSG 2000 (vgl. Art. 4 Z. 2 DSGVO und § 4 Z. 7 DSG 2000), der Verarbeitungsbegriff sollte aber in Kontinuität zur bisherigen Rsp. ausgelegt werden. Siehe dazu näher Pötters/Böhm, in: Wybitul (Hrsg.), Handbuch DSGVO Art. 4 Rz. 11, m.w.N.

Die Abgrenzung der einzelnen Datenverarbeitungen bereitet in der Praxis sehr große Probleme.[4] Eine Hilfestellung bietet dabei etwa die StandardmusterVO.[5] Darüber hinaus können auch bestehende DVR Meldungen als Ausgangslage verwendet werden. Soweit bereits ein Verarbeitungsverzeichnis gem. Art. 30 DSGVO vorliegt, kann auch dieses als Grundlage verwendet werden.

2.3. Zuordnung zur Verarbeitungsprozess-/System-Matrix

Anschließend werden den Datenverarbeitungen die verwendeten IT-Systeme aber auch manuelle Tätigkeiten, wie die Ablage in physischen Archiven zugeordnet. Oft werden nämlich für eine Verarbeitung verschiedene IT-Systeme verwendet. Ergebnis sollte eine **vollständige Matrix** mit den **Datenverarbeitungen** und den verwendeten **IT-Systemen** samt der **analogen Prozessschritte** sein.

2.4. Rechtfertigungsgründe der Datenverarbeitungen

Um die richtige Löschfrist bestimmen zu können, ist es notwendig, die Rechtfertigungsgründe einer Datenverarbeitung zu kennen. Dies ist in Zusammenhang mit der Löschung verarbeiteter Daten deshalb wichtig, da der Widerruf einer abgegebenen Einwilligung und der Widerspruch gegen ein behauptetes berechtigtes Interesse, einen Löschgrund darstellen (sofern kein anderer Rechtfertigungsgrund besteht). In der Verarbeitungs-/Systeme-Matrix müssen die Datenverarbeitungen um die Rechtfertigungsgründe erweitert werden.

2.5. Definieren von Löschfrist und Startzeitpunkt pro Datenverarbeitung

Anschließend muss für jede Datenverarbeitung eine Löschfrist festgesetzt werden. Diese besteht aus zwei Informationen, der sogenannten **Regellöschfrist** und einem **Startzeitpunkt** ab dem die Regellöschfrist zu laufen beginnt.

Zunächst sind also die für eine Datenverarbeitung geltenden **Regellöschfristen** festzulegen. Gibt es keine gesetzlichen Vorgaben, so sind nach bestem Wissen und Gewissen Annahmen zu treffen (und zu dokumentieren). Regellöschfristen können sich insbesondere aus Rechtsvorschriften, Verträgen, fachlichen Anforderungen, Normen und Standards oder Gerichtsurteilen ergeben.

Darüber hinaus ist ein **Startereignis** zu definieren ab dem die Regellöschfrist zu laufen beginnt. Dabei kommen drei Zeitpunkte in Betracht: Ab Erhebung der Daten, ab Ende eines Vorgangs oder ab Ende der Beziehung zum Betroffenen. Aus diesen Merkmalen ergibt sich eine **Löschregel pro Datenverarbeitung.**

2.6. Zuordnung der Datenfelder auf Datenkategorien und Kategorien auf Datenverarbeitungen auf Systemebene

Auf Basis der Verarbeitungs-/Zwecke-Matrix können anschließend einzelne Systeme analysiert werden. Hierbei lohnt es sich mit den Kernsystemen, in denen typischerweise der Großteil der Verarbeitungen stattfinden, zu beginnen. In einem IT-System werden zunächst die Datenfelder eines Systems verschiedenen **Datenkategorien** zugeordnet und damit zusammengefasst. Der Verantwortliche sollte dabei möglichst einheitliche Datenkategorien vorgeben. Anschließend werden die Datenkategorien den einzelnen Datenverarbeitungen zugeordnet.

2.7. Zwischenschritt Beispielmatrix

Nachdem diese Schritte getätigt wurden, sollte *pro IT-System* eine **Löschmatrix** entstehen.

2.8. Feststellung der Löschregel pro Datenkategorie

Da nun die Löschregeln *pro Datenverarbeitung* feststehen, muss abschließend noch die konkrete Löschfrist *pro Datenkategorie* festgelegt werden. Sobald eine Datenkategorie für mehrere Datenverarbeitungen verwendet

[4] Insbesondere werden Datenverarbeitungen von den Mitarbeiterinnen und Mitarbeitern oft mit Computeranwendungen verwechselt.

[5] Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004).

wird, ist diese klarerweise erst dann zu löschen, wenn der letzte Zweck erfüllt wurde. Aus diesem Grund muss jeder Datenkategorie die **längste Löschregel** zugeordnet werden. Gleichzeitig muss sichergestellt sein, dass nur berechtigte Personen Zugriff auf die Daten haben (Rechte- und Rollenkonzept).

3. Weitere Anforderungen zur Löschung

Neben der oben beschriebenen Implementierung eines regulären Lebenszyklus für personenbezogene Daten müssen auch nachfolgende Spezialfälle berücksichtigt werden:

3.1. Widerruf und Widerspruch

Basiert eine Datenverarbeitung auf einer Einwilligung oder einem berechtigten Interesse, ist zu berücksichtigen, dass Betroffene ihre Einwilligung zu bestimmten Datenverarbeitungen widerrufen oder widersprechen. Aus diesem Grund müssen Datenkategorien von Datenverarbeitungen, die auf einer Einwilligung oder einem berechtigten Interesse beruhen, auch aufgrund eines **Triggerevents** (Widerruf oder Widerspruch) gelöscht werden können, natürlich nur insoweit, als keine andere Datenverarbeitung diese Datenkategorien verwendet. Ist dies der Fall muss der Zugriff auf die Daten auf den erforderlichen Personenkreis begrenzt sein.

3.2. Ausnahmen vom Regellöschzyklus

Gleichermaßen muss jedes System eine Möglichkeit bieten, Datensätze von der Löschung auszunehmen, denn so kann es z.B. bei laufenden Gerichtsverfahren notwendig sein, die reguläre Löschung von personenbezogenen Daten auszusetzen. Dazu empfiehlt sich, dass eine Begründung je Fall erstellt und dokumentiert werden muss. Diese Dokumentationsanforderung kann sowohl organisatorisch als auch technisch umgesetzt werden.

3.3. Dokumentationen von Löschungen

IT-Systeme sollten zur Sicherstellung der Vertraulichkeit und Integrität der Daten zudem in einem **Logfile** festhalten, welche Daten (auf Kategorieebene) von der Löschung betroffen waren und zu welchem Zeitpunkt sie gelöscht wurden. Bei diesen Logs handelt es sich oftmals selbst um personenbezogene Daten, die wiederum selbst einer Löschfrist unterliegen.

3.4. Weitergabe von Löschanforderungen an angebundene Systeme

Über Schnittstellen angebundene Systeme müssen entweder automatisch über diese Schnittstelle oder in einem organisatorischen Prozess über die Löschung informiert werden. Darüber hinaus muss der Verantwortliche auch seine Auftragsverarbeiter über die Löschanforderungen informieren. Es sollte in den Auftragsverarbeitungsverträgen vereinbart werden, dass die Auftragsverarbeiter eine Löschbestätigung auf Nachfrage vorweisen können.

Während des gesamten Prozesses, soll stets sowohl die Verarbeitungsebene, wie auch die System-Ebene beachtet werden.[6]

3.5. Archive und Backups

Die ermittelten Löschregeln gelten auch für personenbezogenen Daten in Archiv- und Backup-Systemen.[7] In vielen **Archivsystemen** sind bei der Übertragung Fristen festzulegen, in deren Zeitraum eine Veränderung inklusive einer Löschung der Daten (schon technisch) nicht möglich ist. Dies ist insbesondere bei solchen

[6] D.h. es muss darauf geachtet werden, dass die Löschung sowohl systemseitig als auch prozessseitig und damit IT-Systemübergreifend sauber funktioniert.

[7] Hier ist erfahrungsgemäß essentiell, den Unterschied zwischen Archiven und Backups (Sicherungskopien) zu verstehen. Zweck von **Archiven** ist die strukturierte Ablage zum raschen Wiederauffinden von historischen Daten, an denen keine Änderung mehr vorgenommen werden oder die nicht mehr im aktiven Geschäft benötigt werden. Diese werden häufig aus Performancegründen in Archiven gespeichert. Im Gegensatz dazu dient ein **Backup** als Sicherungskopie und damit ausschließlich der Wiederherstellung von verlorenen/zerstörten/veränderten Daten. Das Backup dient nicht dazu historische Daten aufzubewahren.

Datenkategorien problematisch, die auf ein jederzeit mögliches Triggerevent (z.B. Widerruf oder Widerspruch) gelöscht werden müssen. Hier ist es wichtig diese Frist, in der Daten technisch nicht verändert werden können, entsprechend dem Rechtfertigungsgrund anzupassen, um den Spannungsverhältnis zwischen revisionssicherer Aufbewahrung und datenschutzkonformer Löschung aufzulösen.

Backups für bestimmte Zeiträume sind zulässig und auch datenschutzrechtlich notwendig (Stichwort Verfügbarkeit der Daten). Dafür kann es auch notwendig sein mehrere Generationen von Datensicherungen zu speichern, da nicht vorhersehbar ist, welche Daten von welchem Zeitpunkt eingespielt werden müssen.[8] Allerdings dürfen die Zeiträume für Sicherungskopien ebenfalls nicht länger als notwendig sein. Hier muss gegebenenfalls das Backup-Konzept angepasst werden. Da eine Löschung *in Backups* technisch meist nicht möglich ist, muss in vielen Fällen eine alternative Löschung gefunden werden.[9]

4. Sperren (Rechte- und Rollenkonzept)

Sobald eine Datenkategorie für mehrere Zwecke verwendet wird, ist das Datum erst dann zu löschen, wenn der letzte Zweck erfüllt wurde. Es muss aber dennoch sichergestellt werden, dass nur mehr jene Personen Zugriff auf die personenbezogenen Daten haben, die den Zugriff auch benötigen. Dies geschieht durch Sperren. Sobald ein Zweck wegfällt, wird der Zugriff auf die Daten eingeschränkt. Einschränkung der Verarbeitung bedeutet in diesem Kontext, dass die gesperrten Datensätze nur noch für die übrigen Zwecke von den dafür zuständigen Personen verarbeitet werden dürfen. Das Entsperren von gesperrten Datensätzen muss ebenfalls möglich sein, falls aufgrund fachlicher oder technischer Fehler ein Datensatz irrtümlich gesperrt wurde.

Darüber hinaus müssen bei automationsunterstützt verarbeiteten personenbezogenen Daten, die aus wirtschaftlichen oder technischen Gründen nicht unverzüglich gelöscht werden können, die Datensätze bis zur Löschung gesperrt werden. Wenn ein Datensatz zur Löschung vorgemerkt wurde, muss sichergestellt werden, dass dieser bis zu seiner tatsächlichen Löschung in allen Anwendungen nicht mehr verwendet wird.

5. Zusammenfassung

Das Löschen von personenbezogenen Daten im Unternehmen ist schwierig und komplex. Es steht am Ende der Datenschutz-Reise, da für die Löschung zahlreiche Informationen und Wissen zu den Datenverarbeitungen und der verwendeten IT-Landschaft vorausgesetzt werden. Es müssen vorab viele schwierige datenschutzrechtliche Fragen beantwortet werden, von der Abgrenzung der Datenverarbeitungen über die Klärung der Frage auf welchem Rechtfertigungsgrund eine Datenverarbeitung basiert bis hin zur Kenntnis der einschlägigen Aufbewahrungspflichten, bevor man sich an das Thema «Löschen» wagen kann.

Dennoch lohnt sich die das Thema Löschen für den Verantwortlichen: Neben der Erfüllung der gesetzlichen Bestimmungen bringt die Umsetzung meist eine Verringerung der Kosten, eine Steigerung der Performance und vor allem auch ein besseres Verständnis des eigenen Geschäfts und des eigenen Unternehmens mit sich.

---

8 Oft bemerken Unternehmen einen Angriff oder den Verlust von Daten erst Monate nach dem tatsächlichen Ereignis.

9 Dies kann etwa organisatorisch abgebildet werden, indem ein Prozess vorgesehen wird, bei dem in der Zwischenzeit erfolgte Löschungen oder Sperrungen (im Falle des Wiederherstellens einer Datensicherung) eingearbeitet werden.