

DATENMINIMIERUNG, SPEICHERBEGRENZUNG UND DATENLÖSCHUNG

Informationen zum Datenschutz | September 2023

English version

Einleitung

Im Zusammenhang mit der Speicherung und Löschung von Daten wird häufig darauf verwiesen, dass gelöschte Daten die sichersten Daten seien. Der Ausspruch bezieht sich unter anderem auf die Grundsätze der Datenminimierung gemäß Art. 5 Abs. 1 lit. c) DSGVO und der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e) DSGVO, die wesentliche Prinzipien des Datenschutzrechts darstellen. Schon aus diesen Grundsätzen ergibt sich, dass die Datenverarbeitung auf das notwendige Maß zu beschränken ist und personenbezogene Daten nur so lange gespeichert werden dürfen, wie dies für die verfolgten Zwecke erforderlich ist. Sobald die Daten nicht länger benötigt werden, sind sie nach Art. 17 Abs. 1 DSGVO zu löschen. Darüber hinaus räumt die Vorschrift des Art. 17 Abs. 1 DSGVO Betroffenen ein eigenes Recht ein, die Löschung ihrer Daten von der verantwortlichen Stelle zu verlangen.

Die bei der Speicherung personenbezogener Daten einzuhaltenden Grundsätze der Datenminimierung und Speicherbegrenzung sowie das Thema Datenlöschung werden im Folgenden sowohl aus theoretischer als auch aus praktischer Sicht näher betrachtet.

Speicherung von Daten

Bei der Speicherung von Daten handelt es sich um einen Unterfall der Datenverarbeitung. Wie für jede andere Datenverarbeitung ist auch für die Speicherung personenbezogener Daten zunächst das Vorliegen einer Rechtsgrundlage erforderlich. Es gilt insoweit der in Art. 6 Abs. 1 DSGVO verankerte Grundsatz des Verbots mit Erlaubnisvorbehalt. Eine Datenverarbeitung ist demnach nur dann zulässig, wenn sie auf eine Rechtsgrundlage gestützt werden kann. Vom Grundsatz her kann davon ausgegangen werden, dass Daten nicht gelöscht werden müssen, solange der Verantwortliche eine Rechtsgrundlage für die weitere Speicherung der Daten für sich in Anspruch nehmen kann.

Damit von einer rechtmäßigen Datenverarbeitung ausgegangen werden kann, ist das Vorliegen einer Rechtsgrundlage allein aber noch nicht ausreichend. Darüber hinaus müssen vielmehr zusätzlich die in Art. 5 DSGVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Aus diesen ergibt sich unter anderem, dass personenbezogene Daten nur so lange gespeichert werden dürfen, wie sie benötigt werden. Eine darüber hinaus gehende Speicherung ist in der Regel hingegen unzulässig. Insoweit anzuführen sind vor allem die datenschutzrechtlichen Grundsätze der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e) DSGVO, der Zweckbindung nach Art. 5 Abs. 1 lit. b) DSGVO und der Datenminimierung gemäß Art. 5 Abs. 1 lit. c) DSGVO, wobei sowohl der Grundsatz der Datenminimierung als auch der Grund-

satz der Speicherbegrenzung den Zweckbindungsgrundsatz konkretisieren, gleichzeitig aber auch durch ihn ergänzt werden.

Eine weitere Konkretisierung der Anforderungen ergibt sich aus den Erwägungsgründen der DSGVO. Nach Erwägungsgrund 39 ist die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß zu beschränken und Verantwortliche haben sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, indem sie Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen.

Grundsatz der Datenminimierung

Nach Art. 5 Abs. 1 lit. c) DSGVO muss jede Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“). Dies bedeutet zum einen, dass im Rahmen jeder Datenverarbeitung die Anzahl der verarbeiteten Daten möglichst gering gehalten werden sollte; hierzu gehört auch, die Anzahl der Nutzungen dieser Daten weitestgehend zu reduzieren, etwa in dem Sinn, dass Daten nicht ohne Grund mehrfach ausgewertet werden. Zum anderen sollte auch die Anzahl der von einer Datenverarbeitung betroffenen Personen soweit wie möglich eingeschränkt werden. Der Grundsatz der Datenminimierung verlangt dabei jeweils eine Reduzierung auf das für den in Rede stehenden Zweck notwendige Maß; eine absolute Reduzierung oder Beschränkung der Datenmenge wird demgegenüber nicht gefordert.

Durch entsprechende Technikgestaltung („Privacy by Design“) und durch datenschutzfreundlichen Voreinstellungen („Privacy by Default“) i.S.v. Art. 25 DSGVO kann dem Grundsatz der Datenminimierung ebenfalls Rechnung getragen werden. Der Gedanke des Grundsatzes wird zum Beispiel dadurch aufgegriffen, dass Daten nur zum Lesen bereitgestellt werden und Ausdruck- oder Vervielfältigungsmöglichkeiten demgegenüber eingeschränkt werden.

Beispiel: Werden im Rahmen der Abwicklung eines Gewinnspiels etwa nur der Name und die Adresse des Gewinners benötigt, um den Gewinn versenden zu können, dürfen unter Berücksichtigung des Grundsatzes der Datenminimierung mittels der Teilnahmekarte nicht noch beliebige weitere Kontaktdaten der Teilnehmer, wie Telefonnummer und E-Mail-Adresse, zusätzlich abgefragt werden. Wird eine unmittelbare Kontaktmöglichkeit demgegenüber etwa für die Benachrichtigung des Gewinners, die Organisation der Gewinnübergabe oder Rückfragen benötigt, kann die Abfrage zulässig sein.

Grundsatz der Speicherbegrenzung

Gemäß Art. 5 Abs. 1 lit. e) DSGVO müssen personenbezogene Daten zudem in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“). Der Grundsatz der Speicherbegrenzung zieht also eine zeitliche Grenze für die Verarbeitung personenbezogener Daten. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sind seitens des Verantwortlichen entsprechende Speicher- bzw. Löschfristen hinsichtlich der durch ihn verarbeiteten Daten zu definieren.

Die Anforderungen des Art. 5 Abs. 1 lit. e) DSGVO können seitens des Verantwortlichen in unterschiedlicher Weise erfüllt werden. Maßgeblich ist, dass es unmöglich wird, die zuvor in den zu löschenden Daten verkörpert Information wahrzunehmen. Es besteht zum einen die Möglichkeit, die Daten zu löschen. Zum anderen ist es auch denkbar, den Bezug der Daten zur betroffenen Person aufzuheben. Die Datensätze müssen dabei derart geändert werden, dass die Identifizierung des Betroffenen nicht mehr möglich ist. Liegen die Daten etwa in pseudonymisierter Form vor, kann die Pseudonymliste gelöscht werden. Organisatorische Maßnahmen, wie ein Verbot der Kenntnisnahme, sind demgegenüber nicht ausreichend. Gleiches gilt für das bloße Entsorgen eines Datenträgers im Müll.

Der Grundsatz der Speicherbegrenzung wird zudem durch zahlreiche einzelne Vorgaben der DSGVO konkretisiert. Betroffene müssen etwa nach Art. 13 Abs. 2 lit. a) bzw. 14 Abs. 2 lit. a) DSGVO über die Dauer der Datenverarbeitung informiert werden. Von besonderer Relevanz sind auch das Recht auf und die Pflicht zur Löschung nach Art. 17 Abs. 1 lit. a) DSGVO.

Recht auf Löschung

In Art. 17 Abs. 1 lit. a) DSGVO ist ausdrücklich normiert, dass Daten, die für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, unverzüglich gelöscht werden müssen. Darüber hinaus finden sich in Art. 17 DSGVO noch weitere Gründe, bei deren Vorliegen das verantwortliche Unternehmen zur Datenlöschung verpflichtet ist. Dies sind zunächst der Widerruf einer zuvor erteilten Einwilligung (Art. 17 Abs. 1 lit. b) DSGVO) sowie der erfolgreiche Widerspruch eines Betroffenen gegen eine Datenverarbeitung auf Basis eines berechtigten Interesses (Art. 17 Abs. 1 lit. c) DSGVO). Darüber hinaus müssen Daten auch dann gelöscht werden, wenn die Datenverarbeitung unrechtmäßig ist (Art. 17 Abs. 1 lit. d) DSGVO), z.B. weil es an einer belastbaren Rechtsgrundlage fehlt, die Löschung zur Erfüllung einer gesetzlichen Pflicht erforderlich ist (Art. 17 Abs. 1 lit. e) DSGVO) oder die personenbezogenen Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben wurden (Art. 17 Abs. 1 lit. f) DSGVO).

Die genannten Pflichten zur Löschung personenbezogener Daten aus Art. 17 Abs. 1 DSGVO gelten nicht, wenn einer der Ausnahmetatbestände des Art. 17 Abs. 3 DSGVO erfüllt ist. Daten müssen etwa dann nicht gelöscht werden, wenn sie einer gesetzlichen Aufbewahrungspflicht unterliegen (Art. 17 Abs. 3 lit. b) DSGVO). Schreibt eine andere gesetzliche Regelung die Aufbewahrung vor, ist die weitere Speicherung der Daten auf Basis von Art. 6 Abs. 1 S. 1 lit. c) DSGVO zulässig. Dies gilt auch dann, wenn ein Betroffener in Bezug auf die der Aufbewahrungspflicht unterliegenden Daten seinen Anspruch auf Datenlöschung geltend gemacht hat. Entsprechende Pflichten zur Aufbewahrung von Daten ergeben sich unter anderem aus den handels- und steuerrechtlichen Vorschriften - z.B. § 257 HGB und 147 AO -, dem Arbeits- und Sozialrecht.

Darüber hinaus enthält Art. 17 Abs. 1 DSGVO das Betroffenenrecht auf Löschung. Liegt einer der zuvor genannten Gründe vor, können

betroffene Personen gegenüber der für die Datenverarbeitung verantwortlichen Stelle eine unverzügliche Löschung ihrer Daten verlangen. Es ist sodann zu prüfen, ob das Löschverlangen berechtigt ist und das verantwortliche Unternehmen dem Begehren des Betroffenen nachkommen muss. Die Löschung kann seitens des Verantwortlichen nicht deshalb abgelehnt werden, weil diese einen unverhältnismäßig großen Aufwand für ihn bedeuten würde. Die Prozesse des Unternehmens müssen vielmehr so ausgestaltet werden, dass die Löschrechte nach Art. 17 DSGVO effektiv verwirklicht werden. Die Bearbeitung und Beantwortung von Betroffenenanfragen muss nach Art. 12 Abs. 3, 4 DSGVO unverzüglich, spätestens aber innerhalb eines Monats erfolgen. Kommt der Verantwortliche seiner Löschpflicht nicht nach, kann die Aufsichtsbehörde unter anderem ein Bußgeld gegen das Unternehmen verhängen.

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht, trifft er nach Art. 17 Abs. 2 DSGVO unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten zudem angemessene Maßnahmen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, über das Löschverlangen zu informieren und ihnen mitzuteilen, die Links zu diesen Daten, Kopien oder Replikationen der Daten zu löschen.

Etablierung und Umsetzung eines Löschkonzepts

Da personenbezogene Daten unter Berücksichtigung des Grundsatzes der Datenminimierung und des Grundsatzes der Speicherbegrenzung jedenfalls dann gelöscht werden müssen, wenn der Zweck der Speicherung entfallen ist, sollte eine Definition der anwendbaren Löschfristen und eine Dokumentation der vorgesehenen Abläufe zur Umsetzung der Löschung erfolgen, um die Einhaltung der Vorgaben nachzuhalten. Die datenschutzrechtlichen Grundsätze unterliegen auch der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Aus dieser ergibt sich, dass Unternehmen positiv nachweisen müssen, dass sie die Vorgaben der DSGVO einhalten. Hierzu bietet sich die Erstellung eines Löschkonzepts, in dem dargestellt wird, nach welchen Grundsätzen die Speicherung und Löschung von Daten im Unternehmen organisiert ist, an. In gleicher Weise, wie für die Dauer der Datenhaltung Maßnahmen getroffen werden müssen, die für eine Verfügbarkeit und Wiederherstellung der Daten sorgen, ist auch dafür Sorge zu tragen, dass zum Ablauf der Aufbewahrungszeit für eine Löschung der Daten gesorgt wird.

Es ist insoweit zunächst zu definieren, welche Daten zu welchem Zeitpunkt zu löschen sind. Hierbei ist darauf zu achten, dass die Daten im Unternehmen auch tatsächlich nicht mehr benötigt werden. Bei der Ermittlung der Lösungsreife ist außerdem zu berücksichtigen, dass das Aufbewahrungsinteresse bei alten Daten in der Regel sinkt. In vielen Fällen kann sich das Unternehmen bei der Festlegung der Löschfristen an den Aufbewahrungsfristen und den sonstigen gesetzlichen Vorgaben orientieren. Konkrete Fristen sind im Gesetz zwar nur selten vorgesehen, sie lassen sich allerdings aus den gesetzlichen Regelungen - etwa aus der Verjährung - herleiten.

Anschließend ist festzulegen, auf welche Weise die Löschung erfolgt. Bei klar definierten Aufbewahrungsfristen kommt vor allem eine automatisierte Löschung nach Zeitablauf in Betracht. Hierdurch wird das Risiko gesenkt, dass die Daten versehentlich zu lange aufbewahrt werden. Alternativ ist auch eine manuelle Löschung der Daten, im Rahmen derer ein Mitarbeiter jeweils prüft, ob die in Rede stehenden Daten zu löschen sind, nach festgelegten Zeiträumen denkbar. Hierzu kann zum Beispiel ein regelmäßiger „Lösch- und Aufräumtag“ etwa zu Beginn des Kalenderjahres eingeführt werden. Um die tatsächliche Löschung auch in diesem Fall nachhalten zu können, sollte dokumentiert werden, in welchen Intervallen die Löschung regelmäßig erfolgen soll und ob bzw. in

welchem Umfang die jeweilige Löschung auch tatsächlich erfolgt ist.

Praktischer Umgang mit Löschansprüchen

In der Praxis kommt es häufig vor, dass Betroffene sich an die verantwortliche Stelle wenden und pauschal eine Löschung ihrer Daten unter Berücksichtigung der ihnen nach der DSGVO zustehenden Rechte fordern. Die Betroffenen gehen insoweit häufig davon aus, dass die Verarbeitung ihrer Daten ausschließlich ihrer Entscheidungsgewalt unterliegt. Mit Blick auf die Rechtsgrundlage der Einwilligung ist dies auch zutreffend, da die Daten des Betroffenen ab dem Zeitpunkt des Widerrufs - soweit keine andere Rechtsgrundlage vorliegt - nicht mehr verarbeitet werden dürfen und dementsprechend zu löschen sind. Im Übrigen ist das Löschbegehren des Betroffenen aber nur im Rahmen der Überprüfung der weiteren Datenverarbeitung zu berücksichtigen.

Grundsätzlich empfiehlt es sich, die Anfrage eines Betroffenen präzise und differenziert zu beantworten. Es sollte ihm möglichst genau erklärt werden, welche seiner Daten gelöscht wurden und welche Daten zwar weiterhin - etwa aufgrund von Aufbewahrungspflichten aus dem Handelsrecht - vorhanden sind und aufbewahrt werden müssen, aber nur noch eingeschränkt verarbeitet werden.

Außerdem sollte geprüft werden, was der Betroffene mit seinem Löschbegehren konkret bezwecken möchte. Verlangt ein Kunde etwa die Löschung seiner Daten aus dem Newsletter-Verteiler, möchte er in der Regel in erster Linie erreichen, dass er künftig keinen Newsletter mehr erhält. Ob seine E-Mail-Adresse insoweit auf eine Sperrliste gesetzt oder gelöscht wird, ist für ihn meist zweitrangig.

Kann anhand der konkreten Anfrage nicht eindeutig ermittelt werden, in welchem Umfang der Betroffene eine Löschung seiner Daten wünscht, ist es grundsätzlich zulässig, noch einmal bei dem jeweiligen Betroffenen nachzufragen. Alternativ besteht die Möglichkeit, die Anfrage selbst zu interpretieren. In letzterem Fall geht das Risiko einer Fehlinterpretation allerdings zu Lasten des Unternehmens. Als sinnvoll kann sich deshalb eine Gestaltung erweisen, bei der dem Betroffenen erklärt wird, wie seine Anfrage verstanden wurde und welche Daten auf dieser Basis gelöscht wurden, und

man ihm darüber hinaus die Möglichkeit gibt, sich noch einmal zu melden, soweit er eine Löschung weiterer Daten wünscht.

Unterliegen die Kundendaten einer Aufbewahrungspflicht, dürfen die Daten selbstverständlich weiterhin aufbewahrt werden, auch wenn der Kunde eine Löschung seiner Daten fordert. Dies sollte dem Kunden sodann aber auch mitgeteilt werden, damit er nicht fälschlicherweise davon ausgeht, dass das Unternehmen nicht länger über seine Daten verfügt, was inhaltlich falsch wäre. Verlangt der Kunde etwa die Löschung seines Kundenkontos, in dem auch Transaktionsdaten, die einer Aufbewahrungspflicht unterliegen, hinterlegt sind, könnte ihm insoweit etwa mitgeteilt werden, dass sein Konto deaktiviert wurde und die der Aufbewahrungspflicht unterliegenden Daten gelöscht werden, sobald die für sie geltende Frist abgelaufen ist.

Fazit

Die Speicherung von personenbezogenen Daten erfordert grundsätzlich das Vorliegen einer Rechtsgrundlage. Darüber hinaus müssen auch die weiteren datenschutzrechtlichen Grundsätze bei der Datenverarbeitung eingehalten werden. Durch das Datenschutzrecht werden alle Unternehmen verpflichtet, personenbezogene Daten nur so lange zu speichern, wie dies zur Erfüllung der verfolgten Zwecke erforderlich ist. Anschließend sowie auch in den weiteren in Art. 17 DSGVO aufgelisteten Fällen sind die Daten zu löschen. Neben den allgemeinen Löschpflichten kommt Betroffenen zudem ein eigener Löschanspruch zu. Die Speicherung und Löschung von Daten unterliegt zudem der Rechenschaftspflicht. Die Einhaltung der datenschutzrechtlichen Vorgaben muss dementsprechend dokumentiert werden. Hierzu empfiehlt sich die Erstellung eines Löschkonzepts, in dem der Umgang des Unternehmens mit der Thematik festgehalten wird. Hinsichtlich von Betroffenenanfragen zum Thema Löschung ist auf eine präzise und inhaltlich richtige Beantwortung zu achten. In diesem Kontext ist auch der seitens des Betroffenen verfolgte Zweck in den Blick zu nehmen. Grundsätzlich ist für jeden Einzelfall zu prüfen, ob die Voraussetzungen für eine Löschung vorliegen oder rechtliche Ausnahmetatbestände der Löschung entgegenstehen.

Dr. Sebastian Meyer/Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 113
M sebastian.meyer@brandi.net



Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net

