Datenschutz

Wie löschen Sie Personendaten richtig?

Die Pflicht wie auch das Recht auf Löschung personenbezogener Daten sind im Datenschutzgesetz (DSG)[1] seit Langem verankert. Das Löschen digitaler Personendaten stellt Unternehmen dennoch regelmässig vor zahlreiche Herausforderungen. Mit der anstehenden Revision des Datenschutzgesetzes ist mit noch mehr Löschanfragen zu rechnen.[2] Doch was bedeutet «Datenlöschung» und wie machen Sie es richtig?

Autorin

Anjulie Chiara Bencivenga, BLaw, ist Mitglied des Netzwerks Risikomanagement.

Anjulie Chiara Bencivenga

Personendaten sind jede Art von Information, die sich auf eine bestimmte oder bestimmbare natürliche Person bezieht (bspw. vollständiger Name, Privatadresse, persönliche E-Mail-Adresse). Bestimmbar ist die natürliche Person, wenn sich aus den vorhandenen Informationen Rückschlüsse auf die Identität der Person ziehen lassen.

Wann müssen Sie Personendaten löschen?

Personendaten, die nicht mehr benötigt werden, müssen gelöscht werden. Die Löschung muss endgültig erfolgen. Dabei stellt sich als Erstes die Frage: Ab wann werden die Daten nicht mehr benötigt? Das ist der Fall, wenn der ursprüngliche Zweck, für den Sie die Daten gesammelt haben, erfüllt wurde. Haben Sie bspw. eine Umfrage gestartet, ausgewertet und das entsprechende Projekt abgeschlossen, wurde der Zweck der Datenerfassung erfüllt und die Daten müssen gelöscht werden. Diese Verpflichtung wird neu in Art. 6 Abs. 4 revDSG ausdrücklich festgehalten. In Ausnahmenfällen, wenn bspw. gesetzliche Aufbewahrungspflichten bestehen, müssen Sie die erfassten Daten erst nach Ablauf der gesetzlichen Frist löschen.

Dieser Grundsatz der «Datensparsamkeit» besagt somit, dass der Umfang einer Bearbeitung von Personendaten nicht das Mass überschreiten darf, das erforderlich ist, um den Zweck der Datenbearbeitung zu erfüllen. Der Umfang einer Datenbearbeitung soll demnach stets auf das erforderliche Minimum beschränkt werden.[3] So sinnvoll dieser Grundsatz der «Datensparsamkeit» erscheint, so schwierig ist dessen Umsetzung.

Was das Datenschutzrecht mit «Löschen» meint, ist nicht immer klar. Das bestehende DSG kennt den Begriff des Löschens nämlich nicht und verwendet stattdessen die Begriffe «Vernichten» oder «Anonymisieren». Eine konkrete Definition dieser Begriffe enthält das Gesetz aber ebenfalls nicht. Auch im revidierten Datenschutzgesetz (revDSG) wird dieses Problem weiter bestehen. Die Begriffe «Löschen», «Vernichten» oder «Anonymisieren» werden auch dort nicht einheitlich verwendet.

Löschen, anonymisieren oder doch vernichten?

Daten zu löschen bedeutet nicht, dass es unter keinen Umständen mehr möglich ist, an die gelöschten Daten zu gelangen,

Die effektive Löschung von Daten ist nicht immer ganz einfach.

sondern vielmehr, dass kein Personenbezug mehr hergestellt werden kann. Sowohl eine Anonymisierung von Personendaten als auch eine Vernichtung derselben kann verhindern, dass die betroffene Person re-identifizierbar ist. Welche Variante Sie am besten wählen, hängt davon ab, wie hoch das Interesse an einer Re-Identifikation ist und welche Methoden Ihnen zur Verfügung stehen bzw. mit vernünftigem Aufwand durchführbar sind.

Bei der Vernichtung geht es darum, die Daten rückstandslos zu beseitigen, d.h. die physische Vernichtung oder die irreversible Löschung der Personendaten vorzunehmen. Der Begriff «Vernichten» ist somit stärker als der Begriff «Löschen» und impliziert, dass die Daten unwiederbringlich zerstört werden. Übliche Löschbefehle (bspw. «Papierkorb leeren») oder eine reine Umformatierung stellen noch keine Vernichtung, sondern eine Löschung dar.

Dagegen hat eine korrekt durchgeführte Anonymisierung zur Folge, dass die Daten zwar noch bestehen, sie aber keinen Personenbezug mehr aufweisen. Dabei muss darauf geachtet werden, dass weder der Verantwortliche selbst noch ein Dritter ohne unverhältnismässigen Aufwand einen Personenbezug wiederherstellen kann. Der Vorgang muss auch hier irreversibel und endgültig sein, ansonsten liegt nur eine Pseudonymisierung vor, was nicht ausreicht. Denn bei einer Pseudonymisierung werden Personendaten lediglich unkenntlich gemacht. Dazu werden personenidentifizierende Daten (bspw. Name, Geburtsdatum, Privatadresse) durch ein Pseudonym (bspw. einen Code) ersetzt. Wer die Schlüsselinformationen dazu hat, kann somit die Daten einer bestimmten Person zuordnen (sog. Depseudonymisierung oder Re-Identifizierung).

Eine absolut sichere und irreversible Anonymisierung von Daten ist allerdings heute aus technischer Sicht nicht mehr möglich. Obwohl «Anonymisieren» und «Vernichten» im revidierten Datenschutzgesetz in ihrer Funktion als gleichwertig beurteilt werden (vgl. Art. 6 Abs. 4 revDSG), ist daher – insbesondere bei sensiblen Daten – eine Vernichtung zu bevorzugen.

Die Löschung in der Cloud

Sind digitale Daten «vernichtet», d.h. nicht mehr rekonstruierbar, nachdem der Löschvorgang beendet ist? Dies muss nicht unbedingt der Fall sein, denn in der Praxis ist alles ein wenig komplizierter. Mit forensischen Werkzeugen und Methoden lassen sich gelöschte Daten – auch bei zerstörtem Datenträger – vielfach mit wenig Aufwand wiederherstellen.

Die heutzutage oft genutzten Cloud-Technologien verteilen Ihre Daten in der Regel auf viele verschiedene Server in vielen verschiedenen Ländern. Dabei werden sie repliziert und immer wieder innerhalb der Cloud verschoben. Da es bereits schwierig ist, festzustellen, wo sich die Daten und allfällige Kopien überall befinden, stellen wirksame technische Methoden zur effektiven Löschung von Daten eine Herausforderung dar. Nach dem vermeintlichen Löschvorgang sind Ihre Daten für Sie zwar nicht mehr sichtbar, wahrscheinlich sind aber in einzelnen Rechenzentren, in denen die Cloud betrieben wird, immer noch Kopien davon vorhanden.

Solange diese Daten nicht bspw. durch einen neuen Datensatz überschrieben werden, kann der Cloud-Anbieter Ihre gelöschten Daten auf Anfrage hin auch wiederherstellen (bspw., wenn Sie die Daten unabsichtlich gelöscht haben). Beim Löschen von Daten aus der Cloud haben Sie daher nahezu keine Kontrolle darüber, ob sie auch zuverlässig vernichtet werden. Sie müssen dem jeweiligen

Netzwerk Risikomanagement

Dieser Fachartikel erscheint in einer Beitragsserie, die von Expertinnen und Experten des Netzwerks Risikomanagement beigesteuert wird.

> *www.netzwerk-risikomanagement.ch*

Supprimer correctement les données personnelles

Les données personnelles qui ne sont plus nécessaires doivent être effacées. L'effacement doit être définitif. Ce que le droit de la protection des données entend par «suppression» n'est toutefois pas toujours clair. En effet, les termes d'«effacement», de «destruction» ou d'«anonymisation» ne sont pas non plus utilisés de manière uniforme dans la loi révisée sur la protection des données. La destruction consiste à éliminer les données sans laisser de traces, c'est-à-dire à procéder à la destruction physique ou à l'effacement irréversible des données personnelles. Le terme «destruction» est donc plus fort que le terme «effacement» et implique que les données sont irrémédiablement détruites. Les commandes de suppression usuelles (p. ex. «vider la corbeille») ou un simple reformatage ne constituent pas encore une destruction, mais un effacement. En revanche, une anonymisation correctement effectuée a pour conséquence que les données existent toujours, mais qu'elles ne présentent plus aucun lien avec des personnes. Il faut veiller à ce que ni la personne responsable ni un tiers ne puisse rétablir une référence personnelle sans effort disproportionné. Une anonymisation absolument sûre et irréversible des données n'est toutefois plus possible aujourd'hui d'un point de vue technique. Bien que «anonymiser» et «détruire» soient jugés équivalents dans leur fonction dans la loi révisée sur la protection des données (cf. art. 6 al. 4 LPD révisée), il convient donc de privilégier la destruction – en particulier pour les données sensibles.

L'effacement effective des donnéees est difficile dans le cloud, car les données y sont souvent répliquées et stockées dans différents centres de données. Le cryptage offre une solution. Grâce au cryptage, les données sont rendues illisibles pour des tiers non autorisés. Peu importe où se trouvent les données cryptées, la destruction de la clé de décryptage (et de toutes les copies de cette clé) empêche l'accès à ces données et rend ainsi leur suppression irréversible.

Cloud-Anbieter vertrauen, dass die Daten auch tatsächlich aus allen Datenbanken, Servern, Backups & Co. entfernt werden.

Ein Lösungsvorschlag: Verschlüsselung

Was ist nun eine sichere Methode, um Daten endgültig zu löschen und sicherzustellen, dass diese auch wirklich vernichtet werden, selbst wenn sie sich in der Cloud befinden?

Eine Lösung bietet die Verschlüsselung. Durch die Verschlüsselung werden Ihre Daten für unberechtigte Dritte unlesbar gemacht. Egal wo sich die verschlüsselten Daten befinden, mittels Zerstörung des Entschlüsselungsschlüssels (und aller Kopien dieses Schlüssels) wird der Zugang zu diesen Daten verhindert und damit die Löschung irreversibel.

«Eine absolut sichere und irreversible Anonymisierung von Daten ist heute aus technischer Sicht nicht mehr möglich.»

Solange die Menschheit noch keine leistungsfähigen Quantencomputer entwickelt hat, die Verschlüsselungen erheblich schneller dechiffrieren als herkömmliche Computer, stellt dies die sicherste Methode dar. Wenn Sie also auf Nummer sicher gehen wollen, verschlüsseln Sie Ihre Daten, bevor Sie sie in die Cloud hochladen.

Fazit

Die Löschung von Daten ist nicht so einfach, wie sie vielleicht auf den ersten Blick scheinen mag. Sind gelöschte Daten für Sie als Benutzerin nicht mehr sichtbar, bedeutet das noch lange nicht, dass diese nicht mehr existieren bzw. nicht wiederhergestellt werden können. Wollen Sie wissen, ob die von Ihnen getroffenen Massnahmen ausreichen, müssen Sie die verschiedenen Wiederherstellungsszenarien und deren Wahrscheinlichkeit ermitteln sowie die Risiken beurteilen. ■

(«Vgl. zum Ganzen: Blogbeitrag Datenschutz.law (https://datenschutz.law/ratgeber/wie-loeschst-du-personendaten-richtig)»)

- [1] Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand 1. März 2019, SR 235.1).
- [2] Das revidierte Datenschutzgesetz (revDSG) wird am 1. September 2023 in Kraft treten. Link zum revDSG: https://www.fedlex.admin.ch/eli/cc/2022/491/de.
- [3] In diesem Zusammenhang spricht man auch von der «Verhältnismässigkeit» (vgl. Art. 4 Abs. 2 DSG und Art. 6 Abs. 2 revDSG).