School of Management and Law

Infoletter

Zentrum für Wettbewerbs- und Handelsrecht

Compliance Kompakt

September 2019

«Daten bitte nicht löschen» – Anonymisierung ist nachhaltiger!

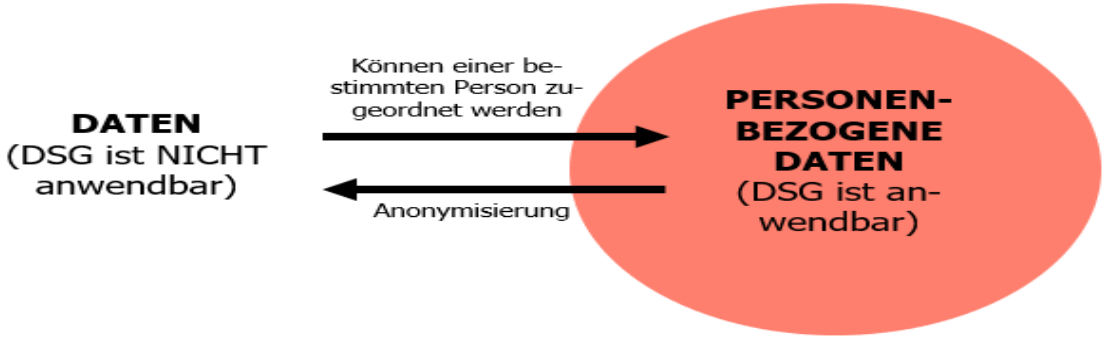
In der Herbstsession 2019 des Schweizer Parlaments (Nationalrat) wird das totalrevidierte Datenschutzgesetz (E-DSG) behandelt (24.9.2019). Wann das E-DSG endgültig verabschiedet wird, kann indes noch nicht gesagt werden. Das E-DSG soll weiter mit dem Europäischen Datenschutzrecht harmonisiert werden und den Veränderungen durch die Digitalisierung Rechnung tragen. Die Bussen sind in der Schweiz zwar tiefer (max. CHF 250'000) als im EU-Recht, es werden aber primär natürliche Personen (in der Regel das Management) mit Strafuntersuchungen ins Recht gefasst. Es kann damit gerechnet werden, dass die Befolgung der Grundsätze zum Datenschutz in den Unternehmen infolge der persönlichen Haftung des Managements besonders hoch sein wird.

Der vorliegende Beitrag befasst sich mit «Data Governance» und der Nutzung wertvoller Datensätze im Unternehmen. Es wird aufgezeigt, wie der **Zweckbindungsgrundsatz im Datenschutzgesetz** durch Planung, Methode und Tools so einsetzbar ist, dass das Wirtschaftsgut «Information» langfristig genutzt werden kann. Statt einer Datenlöschung können die Daten gebraucht werden, um bessere Produkte und Dienstleistungen zu entwickeln.

Personendaten sind Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Nach der Zweckerreichung sind Personendaten wertlos, denn diese dürfen in aller Regel nicht mehr (weiter) bearbeitet werden und sind in der Folge zu löschen. Wenn man die Datenerfassung jedoch von Beginn an richtig plant, kann man auch nach der Zweckerreichung sehr wertvolle Informationen im Unternehmen behalten und Datenanalysen, Preisgestaltungen, Marketingmassnahmen können mit dem vorgestellten Ansatz unter Einbezug auch dieser Daten weiter genutzt werden. Denn die Trennung oder Transformation in «Daten ohne Personenbezug» durch Anonymisierung oder Typologisierung nach Gruppen, Clustern oder «Personas» lösen den Konflikt mit dem Datenschutzgesetz auf. So können die über Jahre gewonnen wertvollen und realen Daten genutzt werden und müssen nicht vernichtet werden. In Art. 5 Abs. 4 E-DSG ist dies (anders als in den Grundsätzen zum Datenschutz in der EU) sogar explizit erwähnt: **«Sie (die Daten) werden vernichtet oder anonymisiert, sobald sie zum Zweck nicht mehr erforderlich sind.»**

Anonymisierung als Form der Löschung

Personendaten müssen gelöscht werden, sobald der Zweck der Speicherung entfällt (Zweckbindung). Eine vollständige Anonymisierung der Daten kommt dabei der Löschung der Daten gleich (vgl. Österreichische-Datenschutzbehörde). Die Methoden und Tools sind seit vielen Jahren aus der Finanzindustrie bekannt, die zum Testen von Finanz-IT-Systemen auf reale Datenstämme angewiesen ist, diese aber aufgrund der strengen Gesetze schon seit jeher nur anonymisiert verwenden darf.



Vorteile der Anonymisierung

Auf «einfache Daten», oftmals auch «**Sachdaten**» genannt, finden die Grundsätze des Datenschutzes keine Anwendung. Nur die Bearbeitungen von **Personendaten** hat nach Massgabe des Datenschutzrechts in der Schweiz (DSG und E-DSG) und in der EU zu erfolgen. Für anonymisierte Personendaten und Sachdaten gelten die Grundsätze des Datenschutzes hingegen nicht. Anonymisierte Daten benötigen keine zusätzlichen Sicherheitsmassnahmen. Sie müssen nicht gelöscht werden und können daher unbegrenzt lange gespeichert und genutzt oder auch ohne Einwilligung an Dritte weitergegeben oder weiterverkauft werden (vgl. https://piwikpro.de/blog/datananonymisierung-fuer-web-analytics-und-marketing/; vgl. Erwägungsgrund 26 der DSGVO).

Nutzen von anonymen Informationen

Viele Analysen und Statistiken sind ohne jeden **konkreten** Personenbezug für das Unternehmen ebenso nützlich. Beispielsweise erheben Unternehmen regelmässig Daten zur Kundenpflege und -bindung. Häufig nutzen sie diese Daten, um das Kundenverhalten zu analysieren sowie Zusammenhänge und Hintergründe des Kaufverhaltens zu identifizieren. Künftige Marketing- und Vertriebstätigkeiten können darauf abgestützt und strategisch geplant werden, ohne dass dafür der konkrete Name, Adresse, Geburtsdatum, Geschlecht usw. der Betroffenen nötig wäre (vgl. datenschutz-praxis.de/anonymisierung, https://www.datenschutz-praxis.de/fachartikel/anonymisierung-und-pseudonymisierung-von-kundendaten/). So können anonyme Daten, Datencluster, Kategorien usw. im Rahmen des sogenannten «Data Driven Marketing» ausgewertet (vgl. http://www.companoo.ch/die-power-der-daten-data-driven-marketing/) und mit aktuellem Verhalten von Kundinnen und Kunden verglichen werden, oder es können etwa Kampagnen aktiv gesteuert werden.

Qualifikation eines Datums zum Personendatum

Informationen werden, wie oben bereits gezeigt, als Personendaten qualifiziert, wenn sie sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG; Art. 4 lit. a E-DSG). Bei der betroffenen Information kann es sich sowohl um Tatsachenfeststellungen als auch um Werturteile handeln. Entscheidend ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen.

Eine Person ist dann bestimmt, wenn sich aus der Information unmittelbar eine bestimmte Person identifizieren lässt. Bestimmbar ist die Person aber auch, wenn aufgrund zusätzlicher, verfügbarer Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung (BGer 1C_285/2009, E 3.2), denn ist nach der allgemeinen Lebenserfahrung nicht damit zu rechnen, dass eine an diesen Daten interessierte Person einen entsprechenden Aufwand auf sich nimmt, ist das Tatbestandselement «Bestimmbarkeit» nicht erfüllt. Daher ist zu würdigen, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, und welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat (BGer 1C_285/2009, E 3.3). Zu beurteilen ist diese Abwägung aus der Sicht des jeweiligen Inhabers der Information (BGer 1C_285/2009, E 3.4.).

Unterschied zwischen Pseudonymisierung und Anonymisierung

Pseudonyme Daten können durch den aktuellen Bearbeiter keiner spezifischen Person zugeordnet werden. Es besteht jedoch für andere, in der Regel für die oder den Verantwortlichen, durch die Einbeziehung weitergehender Informationen (z. B. Mapping-Tabellen) die grundsätzliche Möglichkeit der jederzeitigen Zuordnung (vgl. www.infosec.ch).

Bei anonymen Daten existiert demgegenüber keine Zuordnungsmöglichkeit zu einer spezifischen Person.

Planung und Identifizierung der direkten und indirekt identifizierenden Daten

Um eine Pseudo- oder Anonymisierung durchzuführen, müssen in einem ersten Schritt sowohl direkte als auch indirekte Identifikationsmerkmale im Datensatz selektiert werden. Anschliessend muss bewertet werden, ob die Änderung/Löschung hinsichtlich des Prozesses einer Pseudonymisierung oder Anonymisierung notwendig ist. Es empfiehlt sich, diese Selektion bereits bei der Datenerhebung zu planen und in der sogenannten «Data-Governance» im Unternehmen zu verankern.

1. **Direkte Identifikationsmerkmale**: Alle Daten, welche eine direkte Identifizierung zulassen. Beispiele für direkte Identifikationsmerkmale sind insbesondere Namen, unter denen die Person bekannt ist.
2. **Indirekte Identifikationsmerkmale:** Alle Daten, welche in Verbindung mit anderem indirektem Wissen eine Identifikation ermöglichen, z. B. Personenbezeichner (Steuernummer, Sozialversicherungsnummer, Autokennzeichen usw.); Erscheinungsmerkmale (z. B. Körpergrösse, Haarfarbe, Kleidung, Tätowierungen usw.); biometrische Kennzeichen (z. B. Gesicht, Stimmprofile, Fingerabdrücke); genetische Daten; digitale Zertifikate, welche eine Identifikationsmöglichkeit beinhalten; Identifikationsmerkmale basierend auf elektronischer Kommunikation (z. B. Telefonnummer, Faxnummer, E-Mail, IP-Adresse); demografische Daten (z. B. Religion, Geburtsland, Muttersprache, Vorstrafen); Zuordnungsmerkmale (z. B. Beruf, Funktion, Anschrift, Vorstrafen, Name der Mutter/des Vaters); «Ausreisservariablen» (z. B. seltene Diagnosen;

Super-Luxus-Sportwagen mit nur 10 Exemplaren weltweit) müssen spezifisch bewertet und in der Regel auch ausgeschlossen werden (vgl. Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V., Arbeitshilfe zur Pseudonymisierung/Anonymisierung, 2018, S. 19).

3. **Nicht identifizierende Daten**: Alle anderen Daten, die weder direkte noch indirekte Identifikationsmerkmale darstellen, sind keine Personendaten und unterliegen keinem besonderen Datenschutz.

Methoden der Anonymisierung

Mit den nachfolgenden Methoden zur **Anonymisierung** werden bei **direkten und indirekt identifizierenden Daten** die Anforderungen des Datenschutzgesetzes erfüllt. Zudem können die Daten unbefristeten verwendet oder Dritten zur Verfügung gestellt werden.

1. **Nichtangabe:** Zu schützende Personendaten werden nicht verwendet und weggelassen, z. B. durch Löschung oder Nicht-Exportieren von Spalten einer Tabelle aus einer Datenbank.
2. **Maskierung/Ersetzung**: Zu schützende Daten werden mit einem konstanten oder sich ändernden Wert, Zeichen oder einer Zeichenkette ersetzt.
3. **Clustering** von Daten führt in aller Regel auch zum Ergebnis, dass keine Personendaten vorliegen, indem indirekte Merkmale in Cluster überführt werden, z. B. Altersklassen statt Geburtsdatum, PLZ-Region statt Wohnort, Körpergrösse nach S, M, L usw. Nur wenn im Cluster so wenige Datensätze enthalten sind, dass eine Zuordnung dennoch möglich erscheint oder «Ausreisservariablen» vorliegen, muss die Information auch nach dem Clustering gelöscht oder maskiert werden.
4. **Mischung/Shuffeling**: Hier werden die in den Datensätzen enthaltenen Werte getauscht. Dabei ist zu beachten, dass Informationen, die eine Person eindeutig identifizieren, wie eine Telefonnummer oder eine Kreditkartennummer, zur Auflösung des Personenbezugs zusätzlich weiter verfremdet werden müssen, um einen Personenbezug ausschliessen zu können.
5. **Varianzmethode**: Bei dieser Methode werden Daten, die auf Zahlen basieren, dadurch verfremdet, dass die Zahlenwerte zufällig erhöht oder verringert werden.
6. **Kryptografische Methoden**: Es kommen Verschlüsselungs- und/oder Hash-Algorithmen zum Einsatz. Dabei ist zu beachten, dass kryptografische Eigenschaften wie Blocklänge, Ausgabealphabet und Kollisionen der jeweils verwendeten Methoden Auswirkungen auf das Ergebnis der Anonymisierung haben. Auch darf der Schlüssel nicht bekannt sein.

Fazit

Die im Unternehmen gewonnenen Daten über Kundinnen und Kunden und deren Verhalten müssen auch nach dem neuen Datenschutzrecht **nicht per se gelöscht** werden. Dem Datenschutzrecht ist Genüge getan, wenn nur die identifizierenden Merkmale gelöscht werden. Die nicht identifizierenden Merkmale (keine Personendaten) können jederzeit und insbesondere nach Ablauf der Löschfristen für Personendaten weiterbearbeitet und für künftige Kampagnen oder Marketing und Produktentwicklung genutzt werden. Zudem können anonyme Daten auch an Dritte weitergegeben werden, ohne den Zweckbindungsgrundsatz zu verletzen. Daher sollte dies ein Unternehmen rechtzeitig, das heisst vor der Datenerhebung, ein-

planen, damit die reinen «Sach-Daten» jederzeit auch anderweitig verwendet werden können. Spätestens vor dem Löschen sollte jedoch über eine Anonymisierung der gewonnenen Daten nachgedacht werden.

Die Schweiz ist im neuen totalrevidierten Datenschutzgesetz mit der expliziten Erwähnung der «Anonymisierung gleich Löschung» (Art 4 lit. a E-DSG) fortschrittlich und unternehmensfreundlich, ohne indes den Datenschutz zu vernachlässigen. In der DSGVO der EU findet sich ein solcher Hinweis auch in den Erwägungsgründen nicht.

Volker Dohr, RA (DE), CIA, Dozent