callnet.ch
Swiss Contact Center Association

Revision des Bundesgesetzes über den Datenschutz (Datenschutzgesetz, DSG) per 1. September 2023; Auswirkungen für Callcenter

1. Einleitung

Das revidierte Datenschutzgesetz (DSG) tritt am 1. September 2023 in Kraft. Mit der Revision erfolgen diverse Anpassungen und es entstehen neue Anforderungen an die Unternehmen. callnet.ch orientiert mit diesem Merkblatt seine Mitglieder darüber.

Call- bzw. Contact-Center gibt es in unterschiedlichster Prägung. Sie können Teil des eigenen Unternehmens oder Outsourcing-Partner sein, also Auftragnehmer. Weiter kann unterschieden werden zwischen Callcentern, die primär Anrufe entgegennehmen, weiterleiten oder/und Termine vereinbaren (Inbound), und solchen, die im Auftrag von Unternehmen Anrufe tätigen (Outbound).

Die Grundsätze des Datenschutzgesetzes sind für alle Arten von Callcentern relevant. Die speziellen Bestimmungen für Auftragsbearbeiter gelten jedoch nur für Callcenter, die nicht direkt in das eigene Unternehmen integriert sind. Weiter ist zu beachten, dass die Mitglieder von callnet.ch ausschliesslich in der Schweiz ihren Sitz haben und primär für Schweizer Unternehmen tätig sind.

In diesem Papier sind die Regelungen bezüglich Auftraggeber aus EU/EWR und anderen Ländern nicht berücksichtigt. Dieses Dokument ist auf das revidierte Datenschutzgesetz, welches am 1. September 2023 in Kraft treten wird, ausgerichtet. Mit der Abkürzung «DSG» ist deshalb im Folgenden immer das neue und nicht das aktuell noch gültige Datenschutzgesetz gemeint.

2. Wichtigste neue Bestimmungen des DSG mit Blick auf Callcenter

Auf das revidierte Datenschutzgesetz können sich nur noch *natürliche Personen*, nicht mehr aber *juristische Personen* berufen (Art. 2 Abs. 1 DSG); das hat im Alltag kaum Auswirkungen, da das Gesetz über den unlauteren Wettbewerb (UWG) für Unternehmen zentraler ist und sie schützt. Ein Callcenter kann sich nicht mehr auf das DSG berufen – dies wurde aber auch in der Vergangenheit kaum gemacht.

Bei den Begrifflichkeiten ist *Profiling* (Art. 5 Bst. f DSG) neu dazugekommen. Unter Profiling versteht man «jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen». In Ausnahmefällen kann es vorkommen, dass Callcenter Profilings erstellen. Falls sie Profilings erstellen, müssen sie berücksichtigen, dass sie dies den betroffenen Personen klar kommunizieren. Cookies haben verschiedene Funktionen: Von «First Party Cookies» - diese sichern die ordnungsgemässe Funktionsweise einer Internetseite-, über funktionale Cookies, die beispielsweise eine Sprachauswahl speichern, Performance Cookies, die ein Nutzerverhalten speichern bis zu Marketing Cookies, die auf die vermeintlichen Nutzerinteressen abgestimmte Werbeanzeigen einblenden. Letztere stellen sicherlich ein Profiling dar.

Grundsätze (Art. 6 und 8 DSG): Die Grundsätze des revidierten Datenschutzgesetzes unterscheiden sich inhaltlich nicht von den bis anhin geltenden Grundsätzen. Der Begriff der Erkennbarkeit ist jedoch nicht

mehr zu finden – diese ist Bestandteil von Treu und Glauben, welche auch im neuen DSG explizit festgehalten wird. Neu wird die schnellstmögliche Vernichtung oder Anonymisierung von Daten ausdrücklich stipuliert, sobald diese zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4 DSG). Dies wurde bisher unter die Verhältnismässigkeit subsumiert.

Die Verantwortlichen müssen den Datenschutz durch *Technik* und durch datenschutzfreundliche Voreinstellungen sicherstellen. Dafür wurde ein eigener neuer Artikel geschaffen (Art. 7 DSG). Sie müssen dafür sorgen, dass die Datenbearbeitung streng auf das Minimum beschränkt wird, welches für den Verwendungszweck notwendig ist – ausser, die betroffene Person bestimme etwas anderes.

Eine *Auftragsbearbeitung,* das heisst die Übertragung der Datenbearbeitung durch den Verantwortlichen an einen Auftragsbearbeiter, z.B. einen Spezialisten, ist nach wie vor möglich (Art. 9 DSG). Für den Auftragsbearbeiter gelten dieselben Pflichten wie für den Verantwortlichen; will ein Auftragsbearbeiter einen Dritten beiziehen, muss er dafür die *vorgängige Genehmigung* des Auftraggebers einholen. Entscheidend ist, dass der Auftraggeber insbesondere weiss, wer am Auftrag beteiligt ist – denn die Verantwortung für die Datenbearbeitung verbleibt beim Aufraggeber.

Eine wichtige Neuerung ist die *Datenschutz-Folgenabschätzung* (DSFA) nach Art. 22 DSG. Bei neuen Projekten muss immer hinterfragt werden, ob Personendaten bearbeitet werden. Falls ja, sollte im Rahmen einer sogenannten Schwellenwertanalyse – gelegentlich auch Schutzbedarfsanalyse genannt – eruiert werden, ob diese Bearbeitung ein hohes Risiko für die betroffenen Personen bedeutet (vgl. Checkliste Schutzbedarfsanalyse der Datenschutzstelle des Kantons Zug bzw. Beilage «Schwellenwertanalyse»). Falls die Schwellenwertanalyse positiv ist, muss eine Datenschutz-Folgenabschätzung (DSFA) gemäss Art. 22 DSG durchgeführt werden.

Eine solche DSFA tönt komplizierter als sie ist; auch hier gibt es diverse Hilfsmittel, aktuell von diversen Kantonen, mittelfristig aber auch vom eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Gute Beispiele finden sich bei der Fachstelle für Datenschutz des Kantons St. Gallen (Link) und bei der Datenschutzstelle des Kantons Zug (Link) – aber Achtung: Die kantonalen Gesetze sind für callnet.ch und deren Mitglieder nur anwendbar, wenn sie für eine kantonale Behörde tätig sind.

Es macht Sinn, eine DSFA wie das klassische Risikomanagement durchzuführen; wichtig: Es muss analog ISO 31000 das konkrete Risiko für betroffene Personen eingeschätzt werden.

Anstelle einer Liste von Datensammlungen müssen Unternehmen mit mehr als 250 Mitarbeitenden ein *Verzeichnis der Bearbeitungstätigkeiten* (Art. 12 DSG) erstellen. Die Verantwortlichen und Auftragsbearbeiter führen jeweils ein Verzeichnis ihrer Bearbeitungstätigkeiten. Die für ein Verzeichnis relevanten Punkte sind in Art. 12 klar ausformuliert. Diverse gute Vorlagen finden sich unter anderem bei der FMH, dem Schweiz. Leasingverband oder Treuhand Suisse.

Die *Informationspflicht* bei einer Datenbearbeitung ist erweitert worden (Art. 19 DSG). Sie trifft die Verantwortlichen gemäss dem Gesetz. Betroffene Personen können entweder mittels einer Datenschutzerklärung im Internet, allgemeinen Geschäftsbedingungen (AGB) oder auch mündlich informiert werden. Bei einer mündlichen Information empfiehlt es sich, dies aus Beweisgründen zu dokumentieren. Diese Pflicht umfasst auch jene Daten, welche nicht direkt bei der betroffenen Person beschafft werden. Erfasst ein Callcenter Daten, weil die betroffene Person angerufen hat und beispielsweise einen Reparaturtermin vereinbaren möchte, ist es für die Person allerdings offensichtlich und ohne weiteres erkennbar, dass ihre Daten erfasst werden (Art. 6 Abs. 3 DSG).

Die Informationspflicht liegt beim Verantwortlichen und nicht beim Beauftragten. Insofern müsste ein Callcenter wohl höchstens bei einem Auftrag durch den Auftraggeber diese Informationspflichten wahrnehmen.

Vermehrt kommt es zu Vorfällen durch Hacking, Daten erscheinen im Darknet etc. Dies stellt eine *Verletzung der Datensicherheit* dar, die gemäss Art. 24 DSG zu behandeln ist. Es braucht wiederum eine Risikoabschätzung bezüglich der Risiken der Persönlichkeit und Grundrechte der betroffenen Personen und bei einem hohen Risiko eine Meldung an den EDÖB. Dafür sollte ein Prozess erstellt werden (vgl. auch Vorlage FMH – muss leicht angepasst werden, aber es sind alle relevanten Schritte beschrieben).

Eine Verletzung der Datensicherheit kann oft zu einem medialen Ereignis werden. Es lohnt sich deshalb, den Prozess sowie die wichtigsten Ansprechpersonen zu kennen. Werden IT-Dienstleistungen durch Dritte erbracht, sind diese in den Prozess miteinzubeziehen.

Die *Strafbestimmungen* (Art. 60 ff. DSG) wurden mit der Revision erweitert und der Strafrahmen von Bussen von CHF 10'000 auf CHF 250'000 erhöht. Gleich geblieben ist, dass es sich um Vorsatz-Delikte handelt. Vorsatz bedeutet mit «Wissen und Willen», zumindest muss der Erfolg für «möglich gehalten und bewusst in Kauf genommen» worden sein.

Die Straftatbestände umfassen:

- *Verletzung der Informations-, Auskunfts- und Mitwirkungspflichten*: Eine Datenbeschaffung sollte also nicht heimlich erfolgen. Wird ein Auskunftsbegehren gestellt, ist dieses wahrheitsgemäss und vollständig zu erfüllen. Nicht mehr vorhandene Daten können jedoch nicht herausgegeben werden, ebenfalls kann man sich nicht strafbar machen, wenn versehentlich nicht alle Daten herausgegeben werden; wie oben beschrieben, steht für das Auskunftsrecht der für die Bearbeitung Verantwortliche und nicht der Auftragsbearbeiter in der Pflicht;

- *Verletzung von Sorgfaltspflichten*, indem
    - Daten in ein Land ohne angemessenen Datenschutz bzw. ohne die erforderlichen Garantien oder Verträge/Vertragsklauseln zur Bearbeitung weitergeleitet werden,
    - Daten einem Auftragnehmer übergeben werden, obwohl eine Weitergabe verboten ist oder dieser keine angemessene Datensicherheit gewährleisten kann,
    - Mindestanforderungen an die Datensicherheit nicht eingehalten werden, die man in der Verordnung in Art. 1 ff findet.

  Auch dieser Straftatbestand sollte bei einem normalen, sorgfältigen Umgang mit Personendaten kaum vorsätzlich erfüllt sein.

- *Verletzung der beruflichen Schweigepflicht*: Es ist zu beachten, dass nicht nur bestimmte Berufsgruppen wie beispielsweise Ärzte, Anwälte, Geistliche, Pflegepersonen oder Beamte eine berufliche Schweigepflicht haben, sondern alle Personen in Bezug auf die Bearbeitung von Personendaten, sofern diese Personendaten in Bezug zur beruflichen Tätigkeit stehen. Da auch die Verletzung der beruflichen Schweigepflicht ein Vorsatzdelikt ist, stellt ein ungeschicktes Verhalten in einer Bar, im Zug noch keine Verletzung dar. Vielmehr kann solches Verhalten zu einem Reputationsverlust der Arbeitgeberin/des Arbeitgebers führen.

Zusammengefasst: Das Risiko einer Busse ist sehr klein, sofern man sich vernünftig verhält und nicht absichtlich einer Person schaden möchte.

3. Wichtigste Bestimmungen des DSG mit unveränderter Gültigkeit

Unverändert und unbedingt zu beachten sind die Bestimmungen zur *Datenweitergabe ins Ausland*: Werden Daten einem Auftraggeber ins Ausland weitergeleitet – Achtung: Dies kann auch ein Cloud-Dienstleister sein – ist darauf zu achten, dass die Vorgaben eingehalten sind. Daten dürfen ins Ausland bekannt gegeben werden, wenn die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet. Ansonsten gelten die Regeln gemäss Art. 16 f. DSG).

Wie das bisherige Recht gewährt auch das revidierte Gesetz jeder Person das Recht, vom Verantwortlichen Auskunft darüber zu verlangen, ob Personendaten über sie bearbeitet werden. *(Auskunftsrecht* gemäss Art. 25 ff. DSG). Auch hier empfiehlt es sich, einen Prozess zu definieren, so dass bei einem allfälligen Auskunftsbegehren die notwendigen Unterlagen innert der gesetzlichen Frist von 30 Tagen abgegeben werden können. Dabei ist zu beachten, dass Auskunftsbegehren, bei denen es um Daten des Auftraggebers geht, auch vom Auftraggeber zu bearbeiten sind und nicht vom Callcenter, sofern dieses als Auftragnehmerin agiert.

Weiterhin dürfen auch gegen den Willen der betroffenen Person deren Daten zum Zwecke der Bonitätsprüfung bearbeitet werden. Wichtig ist, dass die Daten nicht älter als 10 Jahre sein dürfen und keine Daten von minderjährigen Personen bearbeitet werden (Art. 31 Abs. 2 Bst. c DSG).

4. Gut zu wissen: weitere Bestimmungen des DSG

Neu muss der Verantwortliche betroffene Personen auch über *automatisierte Einzelentscheide* informieren, die mit einer Rechtsfolge verbunden sind oder die Betroffenen erheblich beeinträchtigen (Art. 21 DSG). Die Relevanz dieser Information nimmt aufgrund der technologischen Entwicklung und der Zunahme automatisierter Entscheide zu. Der Einsatz künstlicher Intelligenz (KI) gewinnt im Alltag an Bedeutung – und kann damit zu neuen Diskriminierungen führen. Dies dürfte für Callcenter aktuell kaum im Vordergrund stehen, mittelfristig jedoch wichtiger werden.

Hierzu als Beispiel: Werden Bewerbende aufgrund der Stichworte im Lebenslauf und in den Arbeitszeugnissen durch ein Programm vorselektioniert, liegt ein automatisierter Einzelentscheid vor, der für die betroffene Person eine Beeinträchtigung zur Folge haben kann; ebenfalls wenn der Entscheid über eine Kreditvergabe automatisiert erfolgt. Kein Ermessensentscheid ist hingegen, wenn beim Bancomat-Bezug aufgrund des Kontostandes ein bestimmter Betrag nicht gegeben wird.

Die Regelung der Weitergabe von Daten (*Datenportabilität*) ist neu dazugekommen und in Art. 28 DSG geregelt. Im Alltag ist sie vor allem bei Plattformen wie Social Media-Kanälen relevant. Dabei handelt es sich primär um Daten, die von der betroffenen Person selbst bekanntgegeben oder mit deren Einwilligung erstellt worden sind.

5. Weiteres Vorgehen

Für das weitere Vorgehen wird ein *Massnahmenplan* empfohlen, welcher folgende Aufgaben umfasst.

Nächste Aufgaben für Callcenter

- *Informationsfluss formalisieren*: Will ein als Auftragnehmer tätiges Callcenter weitere Dritte beiziehen, muss der Auftraggeber vorgängig informiert werden. Dies kann auch zu Beginn des Auftrages erfolgen. Sollen neue Dritte dazu genommen werden, muss der Auftraggeber wieder darüber informiert werden.

- Überprüfen der *Datenschutzerklärung* auf der Internetseite – insbesondere bezüglich der Datenbearbeitung; ist das Callcenter Auftragnehmer ist die Informationspflicht beim Auftraggeber
- Sofern mehr als 250 MA: Erstellen eines Verzeichnisses der *Bearbeitungstätigkeiten*
- Erstellen von *Prozessen* im Umgang mit Auskunftsbegehren und Verletzung der Datensicherheit
- Bei neuen Projekten mittels *Schwellenwertanalyse* prüfen, ob eine DSFA zu erstellen ist.
- *Schulung* und Sensibilisierung der Mitarbeitenden bezüglich Umgangs mit Personendaten; als Grundlage empfiehlt sich ein Datenschutzreglement
- Allenfalls eine Person ernennen, die den «Hut Datenschutz» trägt; die Ernennung einer Datenschutzberaterin/eines Datenschutzberaters im Sinne von Art. 10 DSG ist freiwillig und nur bedingt empfohlen. Die Funktion Datenschutzberaterin/Datenschutzberater erfordert vertiefte Datenschutz-Kenntnisse.
- Prüfen, ob mit Auftragsbearbeitern (insbesondere IT-Dienstleistern) ein *Auftragsbearbeitungsvertrag* (vgl. Muster FMH) erstellt ist
- *Löschen* von nicht mehr benötigten Daten im Sinne von Art. 6 Abs. 4 DSG

6. Fazit

Auf den ersten Blick erscheinen die Anforderungen hoch. Es ist aber zu beachten, dass das revidierte DSG keine Revolution beinhaltet und viele neue (An-)Forderungen mit sich bringt, sondern bisherige Regelungen im Wesentlichen weiterführt. Allerdings gibt es einzelne gewichtige zusätzliche Anforderungen wie die DSFA und eine weitergehende Informationspflicht bei der Bearbeitung von Personendaten. In diesem Sinne gilt:

> „Die schweizerische Gesetzgebung beschränkt sich auf Wichtiges und regelt es generell-abstrakt und technologieneutral. **Der Vorteil dieser Rechtsetzungskultur ist, dass ihre Anwendung nicht in erster Linien Wissen, sondern Denken voraussetzt.**
>
> Mit der Bereitschaft, sich **gedanklich in die Haut der Kundinnen und Kunden zu versetzen** und mit **einer Prise gesundem Menschenverstand** kann jedes Unternehmen mit dem knapp gehaltenen Text von Gesetz und Verordnung vertretbare Lösungen finden.“
>
> Adrian Lobsiger, EDÖB anlässlich eines Referats beim Symposium on Privacy and Security 2023

Abschliessend eine Bemerkung zur Datenschutz-Grundverordnung der EU (DSGVO): Die DSGVO ist kaum anwendbar, da das Marktortprinzip gilt – es sei denn: Man sucht aktiv Kunden im Raum EU/EWR. Dann ist die DSGVO auf diese Kundendaten anzuwenden und eine Bearbeitung braucht immer einen Rechtfertigungsgrund i.S. von Art. 6 DSGVO.

Zürich, im Juli 2023