JANUAR 2024

LEXpress

VOSER
RECHTSANWÄLTE

Notariat
Steuerrecht
Bau- und Planungsrecht
Wirtschafts- und Gesellschaftsrecht
Allgemeines Zivilrecht

www.voser.ch

Datenschutz in KMU: Was gibt es zu tun?

1. Einleitung

Seit dem 1. September 2023 ist das neue Datenschutzgesetz in Kraft. Bei der Umsetzung bestehen in der Praxis grosse Unsicherheiten. Vielen Unternehmen ist unklar, ob etwas gemacht werden muss, und wenn ja, was.

Dieser LEXpress gibt Ihnen einen Überblick über die wichtigsten Handlungsfelder des Datenschutzrechts in der Schweiz. Insbesondere soll dieser Beitrag Unternehmen, welche in der Schweiz tätig sind und die Vorgaben des Schweizer Rechts einhalten müssen, eine Hilfestellung geben. Da die konkrete Ausgestaltung des Datenschutzes stark vom jeweiligen Geschäftsfeld abhängt (bspw. verfügt eine Arztpraxis über völlig andere Daten als ein Bauunternehmen), ersetzt dieser Beitrag die Beratung und Rechtsabklärung im Einzelfall nicht. Die nachfolgenden Themen sind nach Ansicht und Erfahrung der Autoren für Unternehmen, insbesondere KMU, von Relevanz.

2. Grundlagen

2.1 Rechtsgrundlagen

In diesem Beitrag beschäftigen wir uns nur mit der Bundesdatenschutzgesetzgebung (DSG), wobei punktuell Unterschiede und/oder Abgrenzungen zur DSGVO, dem Datenschutzrecht der Europäischen Union (EU), vorgenommen werden. Bereits an dieser Stelle ist zu erwähnen, dass ein wesentlicher Unterschied zwischen dem Schweizer Datenschutzrecht und dem Datenschutzrecht der EU darin besteht, dass die Bearbeitung von Personendaten in der Schweiz grundsätzlich ohne eine Einwilligung der betroffenen Personen zulässig ist, während in der EU als Grundsatz das Verbot der Bearbeitung von Personendaten gilt, ausser es liegt eine Einwilligung der betroffenen Person vor[1].

Nebst dem Bundesdatenschutzgesetz existieren in der Schweiz 25 kantonale Datenschutzgesetze, die den Umgang mit Personendaten durch öffentliche Organe des jeweiligen Kantons regeln. Im Kanton Aargau ist dies das Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) und im Kanton Zürich das Gesetz über die Information und den Datenschutz (IDG). Kantonale und kommunale Behörden unterstehen grundsätzlich nicht der Bundesdatenschutzgesetzgebung, ausser sie handeln privatrechtlich – in diesem Fall ist auf sie das Bundesdatenschutzrecht anwendbar.

2.2 Auf wen ist das DSG anwendbar?

Das Bundesdatenschutzrecht ist anwendbar bei der Datenbearbeitung durch Privatpersonen und Bundesorgane (Art. 2 DSG). Nachfolgend behandeln wir die Datenbearbeitung durch Privatpersonen näher. Unter Privatpersonen des DSG fallen natürliche und juristische Personen des Privatrechts, d.h. KMUs sind Privatpersonen im Sinne des DSG.

[1] PFAFFINGER, in: BAERISWYL/PÄRLI/BLONSKI (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., 2023, Bern, zu Art. 31 N. 19 ff.

2.3 Welche Daten sind geschützt?

Geschützt sind durch das DSG die Daten natürlicher Personen, sogenannte Personendaten, und nicht etwa Sachdaten (Art. 2 Abs. 1 DSG). Somit sind Daten juristischer Personen durch das DSG nicht direkt geschützt (vgl. Art. 5 lit. a DSG), allerdings können juristische Personen den Schutz aus dem allgemeinen Persönlichkeitsrecht ableiten[2].

2.4 Was sind Personendaten?

Gemäss Rechtsprechung des Bundesgerichts liegen Personendaten vor (BGE 136 II 508, E. 3.2), wenn Informationen vorhanden sind, die sich einer bestimmten Person zuordnen lassen und diese somit direkt identifizieren (z.B. der Name). Wenn anhand zusätzlicher Informationen auf eine bestimmte Person geschlossen und mithin ein Bezug zu dieser Person hergestellt werden kann (z.B. Identifikation anhand von Kundenkarten), handelt es sich ebenfalls um Personendaten. Bereits der Schätzwert einer Immobilie kann als Personendaten gelten, auch ohne Angabe der Grundeigentümerin auf dem Formular, da sich diese aus dem Grundbuch ergibt. Sachdaten in Verknüpfung mit Adressen stellen daher grundsätzlich auch Personendaten dar. Der Begriff der Personendaten ist damit sehr weit zu fassen[3].

2.5 Wann liegt eine Datenbearbeitung vor?

Eine Datenbearbeitung im Sinne des DSG liegt ebenfalls sehr niederschwellig vor. Jeder Umgang mit Personendaten gilt als Bearbeiten i. S. v. Art. 5 lit. d DGS. Allein das passive Speichern ist ausreichend, um Datenbearbeitung im Sinne des DSG zu bejahen. Mit anderen Worten müssen Personendaten nicht aktiv verändert und verarbeitet werden, sondern eine blosse Sammlung von z.B. Adressen genügt für die Bejahung einer Datenbearbeitung. Bearbeitungsvorgänge nach DSG sind Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten (vgl. Art. 5 lit. d DSG).

2.6 Worauf muss die datenbearbeitende Person achten?

Die datenbearbeitende Person muss gemäss DSG beachten, dass die Datenbearbeitung rechtmässig ist (keine Verletzung von Rechtsnormen, die direkt oder indirekt den Schutz der Persönlichkeit bezwecken[4]), nicht gegen das Gebot von Treu und Glauben verstösst (keine heimliche Datenbearbeitung), so transparent ist, dass die betroffene Person deren Beschaffung und Zweck erkennen kann, und dass sie verhältnismässig ist. D.h. die Datenbearbeitung darf nur so weit gehen, als dies für den verfolgten Zweck geeignet, erforderlich und den betroffenen Personen zumutbar ist[5]. Damit ist auch gesagt, dass Personendaten vernichtet oder anonymisiert werden müssen, sobald sie für den Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4 DSG). Eine Datenbeschaffung auf Vorrat ist nicht zulässig. In diesem Sinne hielt das Bundesgericht fest: «Nicht existente Daten können nicht missbraucht werden.»[6] Überdies dürfen Daten nur für einen bestimmten Zweck erhoben und so bearbeitet werden, dass es mit diesem vereinbar ist. Schliesslich muss die datenbearbeitende Person sicherstellen, dass die Personendaten richtig sind (z.B. kein falsches Geburtsdatum im Patientendossier-System einer Arztpraxis). Diese datenschutzrechtlichen Grundsätze sind wesentlich, da bei einem Verstoss dagegen die betreffende Datenbearbeitung grundsätzlich als datenschutzwidrig gilt. Liegt ein Rechtfertigungsgrund vor, entfällt die Widerrechtlichkeit der Persönlichkeitsverletzung (Art. 31 DSG)[7]. Typische Rechtfertigungsgründe sind: die Einwilligung (basierend auf angemessener Information)[8] oder überwiegende private oder öffentliche Interessen (bspw. unmittelbarer Zusammenhang mit Abschluss oder Abwicklung eines Vertrags)[9].

2.7. Was passiert, wenn die Vorgaben des Datenschutzes nicht eingehalten werden?

Die Strafbestimmungen des Datenschutzgesetzes zielen primär auf die datenschutzverantwortliche Person, also die natürliche Person (Busse: bis zu CHF 250'000.–, Art. 60 ff. DSG). In Einzelfällen können die Bussen auf juristische Personen überwälzt werden (Widerhandlungen in Geschäftsbetrieben vgl. Art. 64 DSG i. V. m. Art. 6 ff. des Bundesgesetzes über das Verwaltungsstrafrecht). Bestraft werden Verletzungen von Informations-, Auskunfts- und Mitwirkungs-, Sorgfalts- und beruflichen Schweigepflichten (Art. 60 ff. DSG). Auf die eine oder andere Pflicht gehen wir nachfolgend näher ein.

Wie diese Strafbestimmungen gehandhabt werden, ist heute noch ungewiss. Die Praxis wird dies zeigen müssen.

Empfehlung

- *Es ist zu prüfen, ob das DSG im konkreten Fall überhaupt anwendbar ist (d.h.: Liegen Personendaten vor? Werden diese durch Privatpersonen oder Bundesorgane bearbeitet?).*
- *Es ist ein Bewusstsein zu entwickeln, dass jeder Umgang mit Personendaten, unabhängig von eingesetzten Mitteln und Verfahren, eine Datenbearbeitung darstellt (auch passives Speichern).*
- *Die Grundsätze der Datenbearbeitung müssen eingehalten werden (vgl. Art. 6 und 8 DSG), damit keine widerrechtliche Datenbearbeitung vorliegt.*
- *Eine widerrechtliche Datenbearbeitung kann gerechtfertigt sein z.B. durch Vorliegen einer Einwilligung der betroffenen Personen.*
- *Allfällige Strafen treffen nicht primär das Unternehmen, sondern die im Unternehmen für den Datenschutz verantwortliche Person, daher sind die Verantwortlichkeiten intern klar zu regeln.*

[2] MICHAEL WIDMER, Folien zum CAS Datenschutzberater:in, Einführung und rechtliche Grundlagen, S. 50

[3] RUDIN, in: Stämpflis Handkommentar zum DSG, zu Art. 5 N. 2 ff.

[4] DAVID ROSENTHAL, Das neue Datenschutzgesetz in: Jusletter vom 16. November 2020, S. 14

[5] a.a.O.

[6] Urteil des Bundesgericht 1C_273/2020 vom 5. Januar 2021, E. 5.5.3

[7] vgl. PFAFFINGER, a.a.O., zu Art. 31 Rz. 1

[8] vgl. PFAFFINGER, a.a.O., zu Art. 31 Rz 32

[9] Vgl. PFAFFINGER, a.a.O., zu Art. 31 Rz. 52

3. Datenbearbeitungen im Auftrag («Auftragsdatenbearbeitung»)

Von grosser Bedeutung – und vor allem eine Abgrenzungsschwierigkeit – ist die Unterscheidung zwischen Verantwortlichem («Controller») und Auftragsbearbeiter («Processor»). Die Unterscheidung ist relevant, da letztlich der Verantwortliche für die Datenbearbeitung und deren Rechtsfolgen verantwortlich ist. Der Verantwortliche ist diejenige Person, die über Zweck und Mittel der Datenbearbeitung bestimmt und entscheidet, welche Daten zu welchem Zweck erhoben werden.

Beispiel: eine Schreinerei, welche Kunden- und Mitarbeiterdaten (Namen, Adressen, Liegenschaftsdaten mit Personenbezug etc.) in ihren IT-Systemen speichert. Hier ist der Schreiner der Verantwortliche, während der IT-Dienstleister lediglich ein Auftragsbearbeiter ist.

Der Auftragsdatenbearbeiter ist diejenige Person, die im Auftrag des Verantwortlichen Daten bearbeitet (Art. 5 lit. k DSG) und weisungsgebunden ist. Typischerweise geht es bei der Auftragsbearbeitung darum, dass der Verantwortliche Dienstleistungen an einen Dritten auslagert[10]. Beispiele: die IT-Dienstleister, die Zugriff auf die Kundendaten des Verantwortlichen haben und in dessen Auftrag die Daten verwalten, oder ein Treuhandbüro, welches die Buchhaltung und Lohnadministration für den Verantwortlichen besorgt (Zahlungsdaten der Kunden, Lohndaten der Arbeitnehmer).

Der Verantwortliche muss dabei sicherstellen, dass der Auftragsbearbeiter die datenschutzrechtlichen Vorschriften einhält und die Datensicherheit gewährleistet (Art. 9 DSG). Die Datensicherheit wird durch geeignete technische und organisatorische Massnahmen (TOMs) gewährleistet (Art. 8 DSG), bspw. durch Zugriffsbeschränkung, Alarmanlagen, Installieren von gängigen erforderlichen Softwares sowie durch Einsatz von ISMS (Informationssicherheits-Managementsystemen) wie etwa ISO 27000 Series, BSI-200-Familie, CIS Controls (Critical Security Controls) etc.

Nach Art. 9 DSG muss der Verantwortliche mit dem Auftragsdatenbearbeiter eine Auftragsbearbeitungsvereinbarung schliessen. Das DSG sieht dafür kein Formerfordernis vor, d.h., diese Vereinbarungen können konkludent oder mündlich abgeschlossen werden[11], während nach dem Datenschutzgesetz der EU die Auftragsbearbeitungsvereinbarung der schriftlichen Form bedürfen (Art. 28 Abs. 3 EU-DSGVO). Mindestvertragsinhalte gehen aus Art. 12 DSG hervor. Wichtig zu erwähnen ist, dass bei Unterauftragsverhältnissen der Auftragsbearbeiter die Datenbearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen darf (vgl. Art. 9 Abs. 3 DSG). Auftragsbearbeiter, die ihrerseits Auftragsbearbeiter beiziehen, bspw. IT-Dienstleister, haben daher genau zu prüfen, dass die Erlaubnis zur Unterauftragsvergabe vorliegt.

Vorlagen für Auftragsbearbeitungsverträge sind im Internet gut auffindbar, grosse Anbieter im internationalen Umfeld (bspw. im IT-Bereich) stellen häufig Standardformulierungen zur Verfügung.

Die Abgrenzung, ob es sich um einen Verantwortlichen oder einen Auftragsbearbeiter handelt, ist in der Praxis nicht immer einfach und klar. Daher sind im Einzelfall die entsprechenden Vereinbarungen sorgfältig zu erarbeiten und aus Beweisgründen schriftlich festzuhalten.

Empfehlung

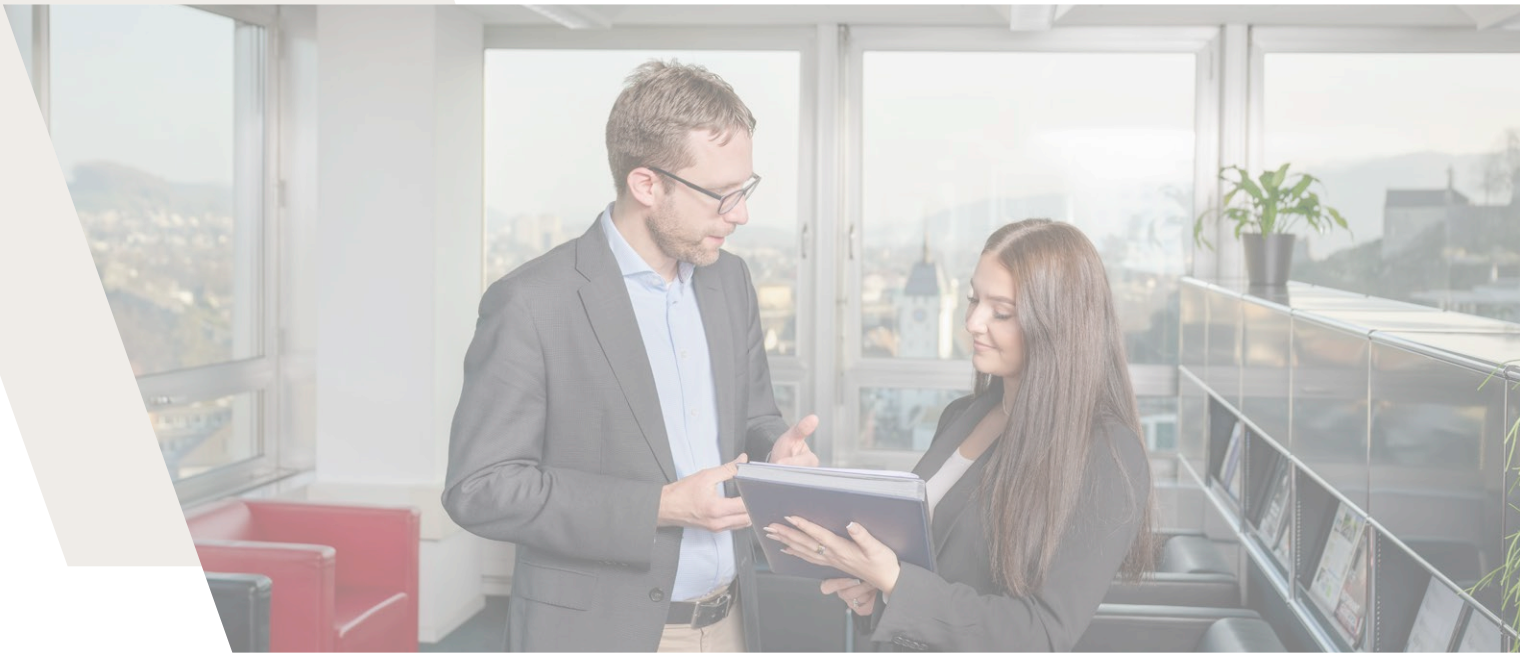
- *Es ist zu prüfen, welche Rolle man hat: Verantwortlicher oder Auftragsdatenbearbeiter?*
- *Die Vertragsgestaltung ist mit Augenmerk auf wichtige Punkte, bspw. Zweck der Bearbeitung, Unterauftragsverhältnisse, Datensicherungsmassnahmen etc., vorzunehmen.*
- *Die Datensicherheit muss mittels geeigneter TOMs gewährleistet sein. Die Frage, welches ISMS angewendet werden soll, ist abhängig von der Grösse der Unternehmen zu beantworten, wobei IT-Fachleute für KMU aus Kostengründen CIS Controls empfehlen, zumal diese auch einfach umsetzbar sind*[12].

4. Datenbearbeitungsverzeichnis

Zu den Pflichten der Datenbearbeiter im neuen DSG ist ein Verzeichnis der Datenbearbeitungstätigkeiten hinzugekommen. Der Mindestinhalt ergibt sich aus dem Gesetz (Art. 12 Abs. 2 und 3 DSG), der Fokus liegt neu auf den Datenbearbeitungsprozessen und deren Dokumentation[13]. Vorab: Für viele KMU dürfte die Pflicht zur Erstellung eines solchen Verzeichnisses entfallen, denn dieses ist nicht erforderlich, wenn weniger als 250 Mitarbeitende beschäftigt und Datenbearbeitungen mit geringem Risiko vorgenommen werden (vgl. Art. 24 Abs. 1 Datenschutzverordnung (DSV). Unabhängig von Mitarbeiterzahlen muss ein Verzeichnis immer erstellt werden, wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden (z.B. Gesundheitsdaten, vgl. Art. 24 Abs. 1 lit. a DSV) oder ein Profiling mit hohem Risiko durchgeführt wird (vgl. Art. 24 Abs. 1 lit. b DSV). Das Verzeichnis muss in diesen Fällen nur für die Datenbearbeitung mit hohem Risiko respektive bei besonders schützenswerten Personendaten erstellt werden, nicht hingegen für allfällige andere Bearbeitungen[14].

Es kann Sinn machen, dass KMU ohne Pflicht zur Verzeichniserstellung eine Art Verzeichnis «light» führen, um überhaupt eine Übersicht über die im Unternehmen anfallenden Datenbearbeitungen zu haben. Eine solche Übersicht kann bspw. die Bearbeitungstätigkeit, die Art der bearbeiteten Daten und die interne Verantwortlichkeit für die Datenbearbeitung abbilden. Denn oft ist den Unternehmen selbst nicht klar, welche Daten überhaupt wie bearbeitet werden.

[10] BAERISWYL, a.a.O., Art. 9 N. 1
[11] BAERISWYL, a.a.O., zu Art. 9 N. 25 ff.
[12] Bernhard Tellenbach, CAS Datenschutzberater:in, Informationssicherheit, Folien 10 ff.
[13] BAERISWYL, a.a.O., zu Art. 12 N. 2
[14] BAERISWYL, a.a.O., zu Art. 12 N. 27 ff.



Empfehlung

- *Es ist zu prüfen, ob ein Datenbearbeitungsverzeichnis erstellt werden muss, d.h. ob mehr als 250 Arbeitnehmende im Unternehmen arbeiten, besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird.*
- *Auch wenn ein Unternehmen von Gesetzes wegen kein Datenbearbeitungsverzeichnis erstellen muss, ist es sinnvoll, sich zumindest eine grobe Übersicht über die im Unternehmen anfallenden Datenbearbeitungen zu verschaffen.*

5. Datenschutzerklärung (DSE)

Das DSG schreibt vor, dass der Verantwortliche die betroffene Person angemessen über die Beschaffung von Personendaten informieren muss (vgl. Art. 19 Abs. 1 DSG). Ausfluss dieser Informations- und Transparenzpflicht ist, dass mittels DSEs über die Beschaffung und Bearbeitung von Personendaten informiert wird. Die Informationspflicht umfasst nicht nur Datenbeschaffungen auf der Website, sondern insbesondere auch im Offline-Kontext, d.h., auch Newsletter, Kundenevents, Bewerbungen, Zahlungsverkehr etc. müssen von der DSE erfasst sein.

Grundsätzlich ist es ausreichend, wenn die Informationen in Form einer DSE auf der Website zur Verfügung gestellt werden, wobei die DSE ohne grossen Aufwand auffindbar sein muss. Die DSE sollte von den AGB respektive den vertraglichen Einwilligungen getrennt sein. Die Information über die Datenbeschaffung und -bearbeitung hat keinen rechtsgestaltenden Charakter wie bspw. die Einwilligung in die AGB[15]. Aus diesem Grund ist davon abzuraten, DSEs zum Vertragsbestandteil zu machen, zumal damit künftig Änderungen nicht einseitig vorgenommen werden können.

Die Einführung von Art. 19 DSG führt zu einer wichtigen Erweiterung der Informationspflicht für private Datenbearbeiter wie KMU. Nach neuem Datenschutzgesetz sind daher auch Private verpflichtet, für jegliche Beschaffungen (auch nicht risikobehaftete) die nötigen Informationen nach Art. 19 DSG in DSEs bereitzustellen[16].

Empfehlung

- *Es ist zu überprüfen, ob eine DSE vorhanden ist und ob diese aktuell ist.*
- *Insbesondere ist genau zu prüfen, ob die DSE alle aktuellen Datenbearbeitungen (sowohl online wie auch offline) abdeckt.*
- *Der Zugang zu den DSEs muss ohne grossen Umstand gewährleistet sein.*

6. Auslandtransfer

Personendaten dürfen grundsätzlich ins Ausland transferiert werden. Der Verantwortliche in der Schweiz hat dafür zu sorgen, dass der Schutz der Persönlichkeit und der Grundrechte der betroffenen Person so gewährleistet ist, wie wenn die Daten in der Schweiz bearbeitet würden (vgl. Art. 16 Abs. 1 DSG). Empfängerstaaten mit einem angemessenen Schutz sind in Anhang 1 der DSV aufgeführt (vgl. Anhang 1, Art. 8 Abs. 1 DSV), Datentransfers z.B. innerhalb des EU-Raums sind grundsätzlich unproblematisch.

Bei einem Datentransfer in ein Drittland ohne angemessenen Datenschutz wie etwa nach Indien müssen zusätzliche Massnahmen zur Sicherstellung eines angemessenen Datenschutzes ergriffen werden. Hier kommen insbesondere vertragliche Garantien sowie die Vereinbarung spezieller TOMs in Betracht. Allerdings kann ein Restrisiko eines unrechtmässigen Zugriffs auf die Daten bzw. einer unrechtmässigen Bearbeitung trotz vertraglicher Garantien und zusätzlicher Massnahmen bestehen bleiben, wenn bspw. die nationale Gesetzgebung im

[15] PÄRLI/FLÜCK, a.a.O., zu Art. 19 N. 22 ff.
[16] PÄRLI/FLÜCK, a.a.O., zu Art. 19 N. 30 ff.

Zielland in bestimmten Fällen den staatlichen Zugriff ermöglicht ohne Wahrung der datenschutzrechtlichen Vorgaben, so zum Beispiel der Foreign Intelligence Surveillance Act (FISA) in den USA. Gestützt auf dieses Gesetz dürfen amerikanische Behörden auf Daten von US-Unternehmen zugreifen, unabhängig davon, wo auf der Welt die Daten abgespeichert sind; dabei kann das betroffene Unternehmen zur Verschwiegenheit verpflichtet werden, d.h., in diesem Fall erfährt der Verantwortliche nicht, dass auf die von diesem zur Bearbeitung zur Verfügung gestellten Daten zugegriffen wurde[17]. Insbesondere Microsoft (aber auch andere Technologieunternehmen) sind im Grundsatz in der ganzen Welt verpflichtet, den US-Behörden Zugriff auf die Daten ihrer Nutzer zu gewähren, wenn die US-Behörden dies verlangen, und zwar ohne Gewährleistung der Verfahrensgarantien nach schweizerischer Rechtsordnung[18]. Unter welchen Voraussetzungen der Datentransfer in die USA möglich ist, ist in der Praxis nicht restlos geklärt[19]. Zumindest bezüglich der Amts- und Berufsgeheimnisse ist derzeit davon auszugehen, dass keine vertraglichen Absicherungen möglich sind, auch wenn solche von den Dienstleistern häufig angeboten werden. Einzig, wenn mit technischen Massnahmen (bspw. durch Verschlüsselung) ein Zugriff verhindert werden kann, ist eine Übertragung zulässig. Private Verantwortliche können betroffene Personen über die mögliche Datenbekanntgabe an US-Behörden informieren und die Zustimmung für eine solche Datenbearbeitung einholen, dann wäre eine Übertragung in eine ausländische Cloud zulässig[20].

Führende Meinungen in der Literatur sind der Ansicht, dass ein risikobasierter Ansatz zulässig und sachgerecht ist und daher die Nutzung von Cloud-Lösungen datenschutzrechtlich grundsätzlich möglich ist[21]. Demgegenüber verfolgen der EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter), aber auch kantonale Datenschutzbehörden einen Nullrisikoansatz und stellen somit den risikobasierten Ansatz in Frage[22]. Nach der hier vertretenen Ansicht sollte im Einzelfall ein risikobasierter Ansatz verfolgt werden, insbesondere wenn keine besonders schützenswerten Personendaten bearbeitet werden und keine Amts- oder Berufsgeheimnisse verletzt werden können. Schliesslich kann es Fälle geben, wo es möglich ist, die Einwilligung des Betroffenen zur entsprechenden Datenübermittlung einzuholen, damit allfällige rechtliche Folgerisiken weiter minimiert werden können.

Empfehlung

- *Es ist zu prüfen, ob der Transfer in ein sicheres oder unsicheres Land erfolgt (vgl. Anhang 1, Art. 8 Abs. 1 DSV).*
- *Bei Cloud-Lösungen sind die vertraglichen Zusicherungen (Speicherort der Daten, Datensicherungsmassnahmen etc.) genau zu prüfen, wobei in der Datenschutzerklärung auf die Cloud-Bearbeitung hinzuweisen ist.*
- *Es ist zu prüfen, ob eine Einwilligung in die Datenbearbeitung in der Cloud sinnvoll und möglich ist.*
- *Die Anwendung des risikobasierten Ansatzes ist u. E. insbesondere bei Fällen ohne Berufs- und Amtsgeheimnisse und ohne besonders schützenswerte Personendaten sinnvoll.*

7. Datenschutz-Folgenabschätzung (DSFA)

Wenn die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, muss der Verantwortliche vorgängig eine DSFA erstellen.

Eine hohes Risiko liegt dann vor, wenn eine umfangreiche Bearbeitung besonders schützenswerter Personendaten oder eine systematische und umfangreiche Überwachung öffentlicher Bereiche vorliegt[23]. Die DSFA ist damit im Kern eine Risikoanalyse, welche die Datenbearbeitungen beschreibt, die Risiken bewertet und Massnahmen zur Risikobehandlung festlegt[24]. Kommt die DSFA zum Schluss, dass die geplante Datenbearbeitung trotz der Massnahmen noch immer ein hohes Risiko für die Betroffenen darstellt, ist der EDÖB zu konsultieren[25].

Die DSFA hat strukturiert und dokumentiert zu erfolgen, wobei keine übermässigen Anforderungen gestellt werden, wenn kein Bedarf nach besonderen Vorkehrungen besteht; in solchen Fällen ist eine einfache Aktennotiz ausreichend[26].

Empfehlung

- *Es ist zu prüfen, ob eine umfangreiche Bearbeitung besonders schützenswerter Personendaten oder die Überwachung öffentlicher Bereiche vorliegt. Wenn ja, ist eine entsprechende DSFA zu erarbeiten.*
- *Die DSFA soll schriftlich erstellt werden, wobei in einfachen Fällen eine einfache Aktennotiz ausreichend sein kann.*

8. Betroffenenrechte

Den Betroffenen stehen nach dem DSG verschiedene Rechte zu. Nachfolgend wird auf die einzelnen Rechte summarisch eingegangen.

8.1 Auskunftsrecht

Gestützt auf das Auskunftsrecht kann der Betroffene vom Verantwortlichen verlangen, ob und bejahendenfalls welche Personendaten von ihm zu welchem Bearbeitungszweck bearbeitet wurden, wie lange die Personendaten aufbewahrt werden und allenfalls woher die Personendaten stammen. Der Betroffene kann auch die Bekanntgabe der Empfänger seiner Personendaten verlangen (Art. 25 Abs. 2 DSG). Das Auskunftsbegehren ist grundsätzlich schriftlich zu stellen und die Auskunft hat kostenlos zu erfolgen, wobei bei unverhältnismässig hohem Aufwand eine Kostenbeteiligung von max.

[17] BAERISWYL, a.a.O., zu Art. N. 70

[18] Vgl. EDÖB, Stellungnahme zur Datenschutz-Risikobeurteilung der Suva zum Projekt Digital Workplace «M365» vom 13. Mai 2022, Ziff. 18

[19] Vgl. Suva, Antwortschreiben zur Stellungnahme EDÖB betr. M365, zu Rz. 18

[20] BAERISWYL, a.a.O., Art. 9 N. 74

[21] https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/, besucht: am 11. Januar 2024

[22] EDÖB, Stellungnahme zur Datenschutz-Risikobeurteilung der Suva zum Projekt Digital Workplace «M365» vom 13. Mai 2022, Ziff. 26

[23] BLONSKI, a.a.O., zu Art. 22 N. 10 ff.

[24] BLONSKI, a.a.O., zu Art. 22 N. 14

[25] BLONSKI, a.a.O., zu Art. 22 N. 22

[26] BLONSKI, a.a.O., zu Art. 22 N. 24

CHF 300.– verlangt werden kann (Art. 19 DSV). Das Auskunftsrecht kann nicht schrankenlos ausgeübt werden, insbesondere kann die Auskunft bei offensichtlich unbegründeten und querulatorischen Gesuchen verweigert werden (Art. 26 Abs. 1 lit. c DSG).

8.2 Recht auf Datenherausgabe und -übertragung

Der Betroffene kann vom Verantwortlichen jederzeit die Herausgabe und Übertragung seiner Personendaten auf Dritte verlangen (z.B. Patientendossier, Personaldossier). Diese Übertragung hat grundsätzlich kostenlos zu erfolgen (Art. 28 Abs. 3 DSG). Bei einer rechtsmissbräuchlichen Ausübung dieses Rechts kann die Datenherausgabe und -übertragung verweigert werden (Art. 29 i. V. m. Art. 26 DSG).

8.3 Recht auf Löschung

Der Betroffene hat das Recht auf Löschung seiner Personendaten und kann vom Verantwortlichen verlangen, dass er alle seine Personendaten für alle Bearbeitungszwecke löscht (Art. 32 Abs. 2 lit. c DSG). Der Verantwortliche hat dem Begehren grundsätzlich Folge zu leisten, da andernfalls eine widerrechtliche Datenbearbeitung vorliegt (Art. 30 Abs. 2 lit. b DSG). Allerdings kann sich der Verantwortliche auf Art. 31 DSG (Rechtfertigungsgründe) berufen und bspw. die Löschung der Personendaten auf gewisse Bearbeitungszwecke beschränken, wenn er für die Weiterbearbeitung der Personendaten für andere Zwecke zum Beispiel gesetzlich verpflichtet ist[27], oder wenn ihn eine gesetzliche Aufbewahrungspflicht trifft (z.B. Spitäler sind gesetzlich verpflichtet, Patientendaten während mindestens zehn Jahren nach Dossierschluss bei sich aufzubewahren).

8.4 Recht auf die Berichtigung und Bestreitungsvermerk

Der Betroffene hat das Recht auf Berichtigung seiner Personendaten (falsches Geburtsdatum im Patientendossier-System). Der Betroffene hat bei Unklarheit darüber, ob die Daten falsch sind oder nicht, ausserdem die Möglichkeit, einen Bestreitungsvermerk zu verlangen[28].

Empfehlung

- *Auf die betroffenen Rechte muss in der DSE verwiesen werden.*
- *Die Verantwortlichkeit für die Sicherstellung der Betroffenenrechte muss klar geregelt sein.*
- *Die Verantwortung für den Datenschutz sollte auf Stufe Geschäftsleitung liegen, wobei es genügt, wenn der Verantwortliche die Geschäftsleitung laufend über den Datenschutz im Unternehmen informiert.*
- *Es empfiehlt sich, auch in kleineren Unternehmen ein Merkblatt oder ein Datenschutzreglement zu definieren, das insbesondere den Umgang mit Anfragen von Betroffenen regelt.*
- *Empfohlen wird die Einrichtung einer personenunabhängigen E-Mail-Adresse (bspw. datenschutz@xyz.ch), auf die in der DSE verwiesen werden muss.*

[27] Rosenthal, a.a.O., S. 52
[28] Rosenthal, a.a.O., S. 53

IHRE SPEZIALISTEN IM DATENSCHUTZRECHT

MLaw Inka Tschudin
Rechtsanwältin,
CAS in Datenschutz

MLaw Dominik Greder
Rechtsanwalt