Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)

15. Januar 2024

INHALTSVERZEICHNIS

1 EINLEITUNG

Dieser Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) ist eine Einführung zu den Risiken, welche die heutigen Informationssysteme aus Datenschutzsicht mit sich bringen, sowie möglichen Lösungen, um mit diesen umzugehen. Er geht auf die wichtigsten Themen des Datenschutzes ein und präsentiert die in Betracht kommenden technischen und organisatorischen Massnahmen wie Verschlüsselung, Anonymisierung, Authentifizierung und so weiter. Der Leitfaden soll dabei helfen, Massnahmen zu realisieren, die einen optimalen und angemessenen Schutz der Personendaten sicherstellen und den aktuellen Regulierungen und Standards entsprechen.

Der Leitfaden richtet sich in erster Linie an Personen, die für Informationssysteme zuständig sind, und sich direkt mit der Verwaltung von Personendaten beschäftigen, ob sie nun Technikerinnen und Techniker sind oder nicht, namentlich Datenschutzberaterinnen und -berater oder Vertreterinnen und Vertreter von Unternehmen mit Sitz ausserhalb der Schweiz. Dieser Leitfaden führt in erster Linie die Pflichten privater Verantwortlicher aus; jedoch finden auch Verantwortliche von Bundesorganen in Abschnitt «Bundesorgane» spezifische sie betreffende Informationen.

Der Leitfaden gliedert sich um acht Schwerpunktthemen: Datenbearbeitung, Rechte und Pflichten, Bundesorgane, Datenschutz, Infrastruktur, Zugriffe und Bearbeitungen, Lebenszyklus der Daten sowie Datenaustausch und -übermittlung. In jedem Abschnitt werden die gesetzlichen Anforderungen beschrieben und die Aspekte dargestellt, die bei der Planung und der Realisierung eines Systems beachtet werden sollten. Dazu werden Massnahmen vorgeschlagen, die als generelle Richtlinien zu verstehen und an die Gegebenheiten des spezifischen Projekts und der Organisation anzupassen sind. Für weitergehende Informationen wird jeweils auch auf die entsprechenden schweizerischen und internationalen Standards verwiesen.

Dieses Dokument ist kein Rechtsratgeber. Zwar werden darin die wichtigsten Vorgaben des Datenschutzgesetzes wiedergegeben, dies aber vor allem zu Informationszwecken. Der Leitfaden soll diese gesetzlichen Vorgaben weder ausführen, kommentieren noch präzisieren. Er ist somit keine Grundlage für die Anwendung oder Auslegung dieser Regeln.

1.1 DATENSCHUTZGESETZ

Dieser Leitfaden stützt sich auf das Bundesgesetz über den Datenschutz (DSG) – insbesondere die Artikel 7 und 8 – und die Verordnung über den Datenschutz (DSV) – insbesondere die Artikel 1–6. In diesen Bestimmungen sind die zentralen Vorschriften festgelegt. Zu beachten ist auch ihr Geltungsbereich, der in den Artikeln 2 und 3 DSG geregelt ist: Das DSG gilt für die Bearbeitung der Daten von natürlichen Personen, die sich in der Schweiz auswirkt, auch wenn die Bearbeitung im Ausland veranlasst wird.

Der Leitfaden verlinkt jeweils auf die relevanten Elemente der Datenschutz-Grundverordnung (DSGVO) und der internationalen Standards. Es sei aber an dieser Stelle präzisiert, dass dieser Leitfaden trotz der häufigen Verweise auf die DSGVO keine vollständige Quelle für die DSGVO-Konformität ist.

Hervorzuheben ist überdies, dass gemäss den Übergangsbestimmungen nach Artikel 69 DSG die Grundsätze des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen (Art. 7), die Datenschutz-Folgenabschätzung (Art. 22) und die Konsultation des EDÖB (Art. 23) nicht auf Datenbearbeitungen anwendbar sind, die vor Inkrafttreten des DSG am

1. September 2023 begonnen wurden, wenn seither weder die bearbeiteten Daten noch der Bearbeitungszweck geändert haben.

Schliesslich sei darauf hingewiesen, dass neben dem DSG auch in der Spezialgesetzgebung Datenschutzbestimmungen zu finden sind, die teilweise von den Vorschriften des DSG abweichen (so zum Beispiel die Artikel 32 ff. des Humanforschungsgesetzes [HFG]). Es ist daher wichtig, dass sich Verantwortliche über Spezialgesetze informieren, die aufgrund ihres Tätigkeitsgebiets allenfalls für sie gelten.

1.2 BEGRIFFE

Um gewisse Konzepte in Zusammenhang mit den organisatorischen und technischen Massnahmen zu unterscheiden, werden in diesem Leitfaden die nachfolgenden Begriffe verwendet. Diese sind spezifisch für diesen Leitfaden und nicht direkt aus dem DSG übernommen.

- Die ***Datensicherheit*** umfasst alle Massnahmen zur Sicherstellung der Vertraulichkeit, der Integrität und der Verfügbarkeit der Daten (z. B. Massnahmen gegen das Abhören oder Verändern von Daten während der Übermittlung).
- Der ***Datenschutz*** umfasst alle Massnahmen zur Gewährleistung der Rechte der betroffenen Personen an ihren persönlichen Daten (z. B. Datensicherheit, Protokollierung, *Privacy by design*).
- Eine **automatisierte Bearbeitung** von Personendaten ist jeglicher Umgang mit Personendaten, der in Systemen zur automatisierten Bearbeitung erfolgt.
- Ein **hohes Risiko** ergibt sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es obliegt den für die Bearbeitung Verantwortlichen, die Persönlichkeit und die Grundrechte der betroffenen Personen zu schützen – und damit auch zu bestimmen, ab wann das Risiko hoch ist, und in diesem Fall die notwendigen Massnahmen zu ergreifen.
  Artikel 22 Absatz 2 Buchstaben a und b DSG nennt zwei konkrete Beispiele, in denen ein hohes Risiko vorliegt (bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten und im Falle einer systematischen Überwachung umfangreicher öffentlicher Bereiche). Diese Aufzählung ist allerdings nicht abschliessend.

Die folgenden Begriffe stammen aus Artikel 5 DSG und werden in diesem Leitfaden analog verwendet:

- **Personendaten:** alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;
- **betroffene Person:** natürliche Person, über die Personendaten bearbeitet werden;
- **besonders schützenswerte Personendaten:**
  - Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
  - Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
  - genetische Daten,
  - biometrische Daten, die eine natürliche Person eindeutig identifizieren,
  - Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
  - Daten über Massnahmen der sozialen Hilfe;
- **Bearbeiten:** jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

- **Bekanntgeben:** das Übermitteln oder Zugänglichmachen von Personendaten;
- **Profiling:** 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;
- **Profiling mit hohem Risiko:** Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;
- **Verletzung der Datensicherheit:** eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;
- **Bundesorgan:** Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist;
- **Verantwortlicher:** private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;
- **Auftragsbearbeiter:** private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

1.3 ALLGEMEINE GRUNDSÄTZE

Das Datenschutzrecht stützt sich auf einige allgemeine Grundsätze, die auf jede Bearbeitung von Personendaten anwendbar sind (Art. 6 DSG). Diese werden im Folgenden in ihren Grundzügen dargestellt – für eine ausführliche Beschreibung wird auf die juristische Fachliteratur verwiesen.

- Personendaten müssen rechtmässig bearbeitet werden (Grundsatz der Rechtmässigkeit). Die Bearbeitung darf demnach keine Rechtsvorschriften verletzen. Dies beschränkt sich nicht auf das DSG, sondern umfasst die Gesamtheit aller Rechtsnormen (insbesondere das Strafrecht wie etwa die Artikel 138 ff. und 179 ff. StGB). Zudem darf die Persönlichkeit der betroffenen Personen nicht verletzt werden, es sei denn, es liegt ein Rechtfertigungsgrund vor (Art. 30 f. DSG). Artikel 31 Absatz 1 DSG nennt als Rechtfertigungsgründe die Einwilligung der betroffenen Person, das Gesetz oder das Vorliegen eines Interesses, welches dasjenige der betroffenen Person überwiegt. In Absatz 2 der Bestimmung ist eine nicht abschliessende Liste solcher Interessen aufgeführt. Dabei ist wichtig zu betonen, dass die genannten Interessen in Betracht fallen, jedoch nicht automatisch als überwiegend gelten. Eine Einzelfallbetrachtung ist notwendig.
- Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein. Verhältnismässig bedeutet, sich für jeden Aspekt der Bearbeitung auf das Nötige zu beschränken: die Beschaffung auf die für den angestrebten Zweck tatsächlich benötigen Daten, den Zugriff auf Personen, die diesen für die Erfüllung ihrer Aufgaben brauchen, aber auch Bekanntgaben oder die Dauer der Aufbewahrung usw.
- Die Person, die Daten bearbeitet, darf mit diesen nicht mehr machen als das, was mit dem angekündigten Zweck vereinbar oder für die betroffene Person zum Zeitpunkt der Beschaffung erkennbar ist (Prinzip der Zweckbindung).
- Wer Personendaten bearbeitet, muss sich über deren Richtigkeit und Vollständigkeit im Hinblick auf den Bearbeitungszweck vergewissern (Grundsatz der Richtigkeit). Sie oder er muss somit in der Lage sein, unrichtige Daten zu erkennen und zu berichtigen.

1.4 FUNKTIONEN

Im Datenschutzbereich finden sich hauptsächlich die folgenden Rollen:

- Der ***Verantwortliche*** ist die private Person oder das Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (vgl. Ziff. 1.2).
- Die Funktion der ***Datenschutzberaterin*** oder des ***Datenschutzberaters*** ist in Artikel 10 DSG definiert (siehe auch die Art. 23 und 25–28 DSV). Die Aufgaben umfassen namentlich die Schulung und Beratung der Verantwortlichen sowie die Mitwirkung bei der Anwendung der Datenschutzvorschriften. Die Person ist ausserdem Anlaufstelle für die betroffenen Personen und die für den Datenschutz zuständigen Behörden.
- Der ***Auftragsbearbeiter*** ist die private Person oder das Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet. Im Allgemeinen gelten für ihn dieselben Grundsätze und Pflichten wie für den Verantwortlichen (Grundsätze nach Art. 6 DSG, *Privacy by design* usw.). Einige Bestimmungen der Datenschutzgesetzgebung regeln spezifisch gewisse Aspekte des Verhältnisses zwischen dem Auftragsbearbeiter und dem Verantwortlichen (namentlich die Art. 9, 24 Abs. 3 und 25 Abs. 4 DSG sowie die Art. 7 und 17 Abs. 2 DSV).
- Der ***Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)*** nimmt Aufgaben der Aufsicht und der Beratung bei Privatpersonen und Bundesorganen wahr. Er führt ausserdem ein öffentliches Register; hierfür sind die Bundesorgane verpflichtet, ihre eigenen Verzeichnisse der Bearbeitungstätigkeiten zu melden (Art. 12 Abs. 4 DSG).
- Der oder die ***kantonale Datenschutzbeauftragte*** nimmt ähnliche Aufgaben auf kantonaler und kommunaler Ebene wahr.

1.5 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Die Risiken, die mit Informationssystemen verbunden sind, lassen sich mit technischen und organisatorischen Massnahmen (Art. 7 und 8 DSG, Art. 3 DSV) verringern. Für die Umsetzung solcher Massnahmen ist der Verantwortliche zuständig.

- ***Technische Massnahmen*** beziehen sich direkt auf den technischen Aspekt des Informationssystems (Anonymisierung, Verschlüsselung, Authentifizierung usw.).
- ***Organisatorische Massnahmen*** sind umfassender und betreffen eher die Umgebung des Systems, die Personen, die es nutzen, und die Art der Nutzung (Berechtigungsregelung, Verzeichnis der Bearbeitungstätigkeiten usw.).

Nur ein Zusammenspiel beider Arten von Massnahmen verhindert die Vernichtung oder den Verlust von Daten, aber auch Irrtümer, Fälschungen, unberechtigten Zugang usw. Diese Massnahmen sind während des ganzen Lebenszyklus der in einem Informationssystem enthaltenen Daten zu implementieren und müssen auf jeder Stufe des Systems greifen.

1.6 HILFSMITTEL

Das DSG bietet vor allem zwei Instrumente, die den Verantwortlichen als Orientierungshilfe dienen und sie bei der Erfüllung ihrer Pflichten unterstützen sollen:

– Verhaltenskodizes (Art. 11 DSG, Art. 12 DSV): Dabei handelt es sich um Sammlungen bewährter Verfahren im Bereich des Datenschutzes, die von den Berufs-, Branchen- und Wirtschaftsverbänden, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind, entwickelt worden sind. Die Verbände können

ihren Verhaltenskodex dem EDÖB vorlegen, der dazu Stellung nimmt. Die Stellungnahme wird veröffentlicht. Es handelt sich dabei nicht um eine Verfügung des EDÖB, mit der er den Verhaltenskodex genehmigt oder ablehnt, sondern um eine einfache Stellungnahme.

– Zertifizierungen (Art. 13 DSG): Die Hersteller von Datenbearbeitungssystemen oder -programmen sowie die Verantwortlichen und Auftragsbearbeiter können ihre Produkte von einer anerkannten unabhängigen Zertifizierungsstelle zertifizieren lassen. Mit der Zertifizierung belegen sie, dass sie die Anforderungen des DSG erfüllen.

Neben dem, dass sie die Konformität mit den Datenschutzanforderungen gewährleisten, haben diese Hilfsmittel noch weitere Vorteile: Nach Artikel 22 Absatz 5 DSG kann der Verantwortliche von der Erstellung einer Datenschutz-Folgenabschätzung nach Artikel 22 DSG absehen, wenn er einen Verhaltenskodex befolgt oder über eine Zertifizierung verfügt. Zudem können diese Instrumente eine Bekanntgabe von Daten ins Ausland ermöglichen, wenn der fragliche Staat selbst keinen angemessenen Datenschutz gewährleistet (Art. 16 DSG und Art. 12 DSV).

Standards					Massnahmen zu ...	Gesetze/Verordnungen			Anderes
COBIT	BSI	CH-MS	ISO 27001	ISO 27701		DSG	DSV	DSGVO	EDPB[1]
X	X	X	X		**Datenaustausch und -übermittlung (extern)**	X	X	X	
X	X	X	X		**Bearbeitung (intern)**	X	X	X	
X	X	X	X		**Infrastruktur**	X	X	X	
				X	**Daten an sich**	X	X	X	X
					Betroffene Personen	X	X	X	X

Datensicherheit

Datenschutz

Tabelle 1: Massnahmen nach Element der Datenbearbeitung, zugrunde liegende Gesetze sowie Standards, welche die Massnahmen abdecken.[2] Der Klarheit halber wird die in diesem Leitfaden gemachte Unterscheidung zwischen Datenschutz und Datensicherheit (vgl. Ziff. 1.2) nochmals verdeutlicht.

Der «Minimalstandard zur Verbesserung der IKT-Resilienz» (CH-MS [1]) ist ein einfacher praktischer Leitfaden, der auf die anderen Standards (ISO [2], COBIT [3], BSI [4] und NIST [5]) verlinkt. In den nachfolgenden Kapiteln wird für ergänzende Informationen jeweils auf den CH-MS verwiesen.

[1] *European Data Protection Board*, vormals «Artikel-29-Gruppe».

[2] Dieser Leitfaden befasst sich mit der Bearbeitung von Personendaten. Auf die Bearbeitung anderer Arten von Daten wird nicht eingegangen. Diese kann anderen Gesetzen unterstehen, welche in diesem Leitfaden nicht erwähnt sind.

2 DATENBEARBEITUNG

Den Verantwortlichen obliegen der Schutz und die Sicherheit der Personendaten, die sie bearbeiten oder bearbeiten lassen. Das DSG verpflichtet sie namentlich zwei spezifische Instrumente umzusetzen, wenn die Voraussetzungen erfüllt sind: die Datenschutz-Folgenabschätzung und das Register der Bearbeitungstätigkeiten. Ausserdem bestehen für Verantwortliche unter Umständen Meldepflichten im Falle einer Verletzung der Datensicherheit oder die Pflicht, eine Vertretung in der Schweiz zu bezeichnen, wenn sie selbst im Ausland ihren Sitz oder Wohnsitz haben. Mit diesen Elementen befasst sich das folgende Kapitel.

Weitere Pflichten der Verantwortlichen werden in den Abschnitten «Rechte und Pflichten» und «Datenschutz» behandelt.

2.1 DATENSCHUTZ-FOLGENABSCHÄTZUNG

Artikel 22 DSG beziehungsweise Artikel 35 DSGVO verlangt eine Datenschutz-Folgenabschätzung, «wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann».

Nach Artikel 23 DSG ist der Verantwortliche zudem verpflichtet, den EDÖB zu konsultieren, wenn die Folgenabschätzung zeigt, dass trotz der vorgesehenen vorbeugenden Massnahmen ein hohes Risiko besteht.

Die Erstellung einer Datenschutz-Folgenabschätzung (DSFA oder PIA für *Privacy Impact Assessment*) durch den Verantwortlichen bezweckt:

- die frühzeitige Erkennung und Behebung von datenschutzrelevanten Problemen, wodurch die Komplexität und die Kosten der Problemlösung tiefgehalten werden;
- den Nachweis der Einhaltung der Datenschutzgrundsätze, einschliesslich in Fragen des Auskunftsrechts der betroffenen Personen;
- den Nachweis der Konformität der Bearbeitung, namentlich bei der Konzeption des Systems, den Risikominderungsmassnahmen und den umgesetzten Kontrollen, um sicherzustellen, dass die Rechte der betroffenen Personen gewahrt werden;
- die Abklärung, ob die Bearbeitung dennoch Risiken im Sinne von Artikel 23 Absatz 1 DSG für die Persönlichkeit oder die Grundrechte der betroffenen Personen birgt.

Die DSFA ist ein wichtiges Instrument des DSG. Sie liefert Informationen zur Art und Weise, wie die Risiken beurteilt wurden, und zu den vorgesehenen Massnahmen zum Umgang mit ihnen. Diese Elemente sind ausserdem besonders nützlich für die Bewältigung und Evaluation von Vorfällen, wie einer Verletzung der Datensicherheit. Auf der Website des EDÖB ist ein Merkblatt zur DSFA publiziert[3]. Auch CNIL[4], ICO[5] und EDPB[6] stellen auf ihren Websites Leitfäden und Vorlagen zur Verfügung.

In diesem Abschnitt werden die folgenden Fragen beantwortet:

- Wann muss eine DSFA durchgeführt werden?
- Unter welchen Voraussetzungen ist eine DSFA freiwillig?
- Wie wird eine DSFA durchgeführt?

[3] Datenschutz-Folgenabschätzung (admin.ch)
[4] Privacy Impact Assessment (PIA) | CNIL
[5] Data protection impact assessments | ICO
[6] ARTICLE29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)

2.1.1 Pflicht zur Erstellung einer DSFA

Vor Beginn einer Datenbearbeitung muss der Verantwortliche eine Folgenabschätzung erstellen, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann. Zu beachten ist, dass gemäss den Übergangsbestimmungen (Art. 69 DSG) auch eine Folgenabschätzung für Bearbeitungen erstellt werden muss, die vor Inkrafttreten des neuen DSG begonnen wurden, wenn der Bearbeitungszweck ändert oder neue Daten beschafft werden.

Artikel 22 Absatz 2 DSG präzisiert, dass sich das hohe Risiko aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergibt. Ein solches Risiko liegt namentlich bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten vor oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

Dahingegen müssen private Verantwortliche keine DSFA erstellen, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind (Art. 22 Abs. 4 DSG).

2.1.2 Ausnahmen von der Pflicht zur Erstellung einer DSFA

Eine DSFA ist in der Regel mit einem hohen Aufwand verbunden. Für Unternehmen, die regelmässig Datenbearbeitungen vornehmen, die eine DSFA erfordern, kann es daher interessant sein, Massnahmen in Betracht zu ziehen, dank derer von einer DSFA abgesehen werden kann.

Artikel 22 Absatz 5 DSG sieht für private Verantwortlichen zwei Möglichkeiten vor:

Zertifizierung: Der Verantwortliche kann ein System, ein Produkt oder eine Dienstleistung einsetzen, das oder die nach Artikel 13 DSG zertifiziert ist. Die Zertifizierungen werden durch anerkannte unabhängige Zertifizierungsstellen erteilt.

Verhaltenskodex: Er kann ausserdem einen Verhaltenskodex im Sinne von Artikel 11 DSG befolgen, der die folgenden drei Voraussetzungen erfüllt: Er beruht selbst auf einer DSFA; er sieht Massnahmen zum Schutz der Persönlichkeit und der Grundrechte vor; er wurde dem EDÖB vorgelegt. Die Verhaltenskodizes werden von Berufs-, Branchen- und Wirtschaftsverbänden erstellt, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind.

Wird ein solches Instrument eingesetzt, so ist die Ausnahme von der Pflicht gerechtfertigt, weil der Verantwortliche dadurch in einer Umgebung arbeitet, deren Datenschutzkonformität bereits erwiesen ist.

2.1.3 Datenschutzberaterin oder Datenschutzberater

Zu beachten ist auch die Funktion der Datenschutzberaterin oder des Datenschutzberaters (Art. 10 DSG und Art. 23 DSV). Ergibt sich aus der DSFA, dass trotz der vorgesehenen Massnahmen noch grosse Risiken vorhanden bleiben, so muss der Verantwortliche normalerweise die Stellungnahme des EDÖB einholen (Art. 23 DSG). Auf die Konsultation des EDÖB kann aber verzichtet werden, wenn eine «qualifizierte» Datenschutzberaterin oder ein «qualifizierter» Datenschutzberater konsultiert wird. «Qualifiziert» heisst, dass die folgenden Voraussetzungen (Art. 10 Abs. 3 DSG) erfüllt sind:

- Die Person übt ihre Funktion gegenüber dem Verantwortlichen fachlich unabhängig und weisungsungebunden aus. Dies bedeutet nicht zwingend, dass es sich um eine externe Person handeln muss. Falls sie intern ist, müssen jedoch organisatorische Massnahmen getroffen werden, die ihre Unabhängigkeit garantieren.
- Sie übt keine Tätigkeiten aus, die mit ihren Aufgaben als Datenschutzberaterin oder -berater unvereinbar sind (Interessenkonflikte).
- Sie verfügt über die erforderlichen Fachkenntnisse.
- Der Verantwortliche veröffentlicht ihre Kontaktdaten und teilt diese dem EDÖB mit (der hierfür ein Meldeportal bereitstellt)[7].

Massnahmen:

- Abklären, ob zertifizierte Instrumente existieren, die den Bedürfnissen gerecht werden, und gegebenenfalls den Aufwand für deren Nutzung und den Aufwand für die wiederholte Erstellung von DSFA vergleichen.
- Abklären, ob ein Verhaltenskodex existiert, der den Voraussetzungen gerecht wird, und gegebenenfalls den Aufwand für dessen Anwendung und den Aufwand für die wiederholte Erstellung von DSFA vergleichen.
- Die Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters in Betracht ziehen, die oder der die Voraussetzungen nach Artikel 10 Absatz 3 DSG erfüllt.

2.1.4 Bestandteile einer DSFA

Nach Artikel 22 Absatz 3 DSG muss eine DSFA Folgendes enthalten:

– eine Beschreibung der geplanten Bearbeitung;
– eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen;
– die Beschreibung der vorgesehenen Massnahmen zur Minimierung dieser Risiken;
– eine Bewertung des Restrisikos nach Berücksichtigung der getroffenen Massnahmen zur Risikobegrenzung (Art. 23 DSG).

Die DSFA ist das Instrument, auf dem das Risikomanagement basiert. Sie muss deshalb mit der notwendigen Sorgfalt und Genauigkeit erstellt werden. Mit einer gut gemachten DSFA können nicht nur Risiken erkannt und reduziert oder beseitigt werden – sie ermöglicht auch eine bessere Reaktion im Ereignisfall.

2.2 VERZEICHNIS

Verantwortliche sind grundsätzlich verpflichtet, ein Verzeichnis der Bearbeitungstätigkeiten zu führen (Art. 12 Abs. 1 DSG). Diese Pflicht haben auch Auftragsbearbeiter.

Verantwortliche

Nach Artikel 12 Absatz 2 DSG muss das Verzeichnis des Verantwortlichen mindestens folgende Informationen enthalten:

– die Identität des Verantwortlichen;
– den Bearbeitungszweck;
– eine Beschreibung der Kategorien betroffener Personen;
– eine Beschreibung der Kategorien bearbeiteter Personendaten;

[7] Meldeportal: dpo-reg.edoeb.admin.ch

– die Kategorien der Empfängerinnen und Empfänger;
– wenn möglich die Aufbewahrungsdauer der Personendaten; andernfalls die Kriterien zur Festlegung dieser Dauer;
– wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8 DSG;
– falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien (Art. 16 Abs. 2 DSG), wie im Abschnitt Datenbekanntgabe ins Ausland ausgeführt.

Auftragsbearbeiter
Das Verzeichnis der Auftragsbearbeiter muss mindestens folgende Angaben enthalten (Art. 12 Abs. 3 DSG):

– die Identität des Auftragsbearbeiters;
– die Identität des Verantwortlichen;
– die Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden;
– wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8 DSG;
– falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien (Art. 16 Abs. 2 DSG), wie im Abschnitt Datenbekanntgabe ins Ausland ausgeführt.

Ausnahmen
Unternehmen und andere privatrechtliche Organisationen, die am 1. Januar eines Jahres weniger als 250 Mitarbeitende beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, es sei denn (Art. 12 Abs. 5 DSG und Art. 24 DSV):

– es werden besonders schützenswerte Personendaten in grossem Umfang bearbeitet;
– es wird ein Profiling mit hohem Risiko durchgeführt.

Massnahmen:

- Regelmässig überprüfen, ob die Datenbearbeitungen (und die Anzahl Mitarbeitende) zur Führung eines Verzeichnisses verpflichten.
- Wenn eine neue Datenbearbeitung geplant wird, die Pflicht zur Führung eines Verzeichnisses von Anfang an mitberücksichtigen, um die Datenerfassung darin zu vereinfachen.

2.3 MELDUNG VON VERLETZUNGEN

Wenn es trotz der umgesetzten Schutzmassnahmen zu einer Verletzung der Datensicherheit kommt, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, muss der Verantwortliche diese dem EDÖB so rasch als möglich melden (Art. 24 Abs. 1 DSG). Ereignet sich die Verletzung bei einem Auftragsbearbeiter, so muss dieser ebenfalls so rasch als möglich den Verantwortlichen verständigen (Art. 24 Abs. 3 DSG).

Wie in Artikel 24 Absatz 2 DSG präzisiert ist, muss die Meldung an den EDÖB mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen nennen. Zudem muss der Verantwortliche die betroffene Person informieren,

wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Weitere Einzelheiten zu den Modalitäten der Meldung sind in Artikel 15 DSV geregelt.

Der Verantwortliche kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn (Art. 24 Abs. 5 DSG):

- dies aufgrund überwiegender Interessen Dritter erforderlich ist;
- der Verantwortliche einer gesetzlichen Geheimhaltungspflicht untersteht;
- die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert; oder
- die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.

Massnahmen:

- Sich über bewährte Verfahren zum Schutz vor Hackern informieren. Einige finden sich in diesem Leitfaden in den Abschnitten Zugriff und Bearbeitungen und Datenaustausch und -übermittlung. Hilfreich sind auch Fachdokumentationen zu bewährten Verfahren[8] sowie spezialisierte Unternehmen, die direkt bedarfsgemäss beraten können.
- Eine Dokumentvorlage oder ein Protokoll für den Ereignisfall vorbereiten, damit die Verletzung der Datensicherheit ohne Verzögerung auf dem Meldeportal DataBreach gemeldet werden kann.[9]
- Über ein klares Protokoll für den Umgang mit solchen Zwischenfällen verfügen, in dem auch eine realistische Vorgehensweise zur Kontaktierung der betroffenen Personen vorgesehen ist.

2.4 VERANTWORTLICHE IM AUSLAND

Die Artikel 14 und 15 DSG betreffen Verantwortliche mit Sitz oder Wohnsitz (das heisst Unternehmen oder natürliche Personen) im Ausland. Diese müssen eine Vertretung in der Schweiz bezeichnen, wenn sie Personendaten von Personen in der Schweiz bearbeiten und die Datenbearbeitung die folgenden Voraussetzungen erfüllt:

- Die Bearbeitung steht im Zusammenhang mit dem Angebot von Waren und Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz.
- Es handelt sich um eine umfangreiche Bearbeitung.
- Es handelt sich um eine regelmässige Bearbeitung.
- Die Bearbeitung bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich.

Der Verantwortliche muss den Namen und die Adresse der Vertretung veröffentlichen, diese dient als Anlaufstelle für die betroffenen Personen und den EDÖB. Die Vertretung muss ein Verzeichnis, ähnlich wie jenes des Verantwortlichen, führen (Art. 15 Abs. 1 DSG) und dem EDÖB auf Anfrage die im Verzeichnis enthaltenen Angaben mitteilen. Auf Anfrage erteilt sie auch den betroffenen Personen Auskünfte darüber, wie sie ihre Rechte ausüben können.

[8] Small Business Guide: Cyber Security - NCSC.GOV.UK
[9] EDOEB DataBreach (admin.ch)

Massnahmen:

- Ein Verzeichnis führen, wie im Abschnitt Verzeichnis beschrieben, und die Informationsübermittlung protokollieren.
- Eine Mitarbeiterin oder einen Mitarbeiter ausbilden oder eine qualifizierte Vertretung finden, die oder der die Aufgaben nach Artikel 14 und 15 DSG wahrnimmt, namentlich in Zusammenhang mit den Rechten der betroffenen Personen (Rechte und Pflichten).

3 RECHTE UND PFLICHTEN

Jede Datenbearbeitung muss die allgemeinen Grundsätze gemäss Artikel 6 DSG beachten. Diese werden durch Rechte konkretisiert, die den betroffenen Personen zustehen. Namentlich sind dies:

- *das Recht, über die Datenbeschaffung informiert zu werden (Art. 19–21 DSG);*
- *das Auskunftsrecht und das Recht auf Datenherausgabe (Übertragbarkeit; Art. 25–29 DSG);*
- *das Recht, eine widerrechtliche Bearbeitung zu verhindern, namentlich indem die Beendigung der Bearbeitung, die Berichtigung unrichtiger Daten oder auch die Vernichtung der Daten verlangt wird (Art. 32 und 41 DSG).*

In der DSGVO sind diese Aspekte in den Artikeln 13–20 geregelt.

Jede Person, deren Personendaten bearbeitet werden, hat gewisse Rechte in Bezug auf die Bearbeitung, und die Verantwortlichen müssen in der Lage sein, die Wahrnehmung dieser Rechte zu garantieren. Dieser Abschnitt beschreibt die verschiedenen Rechte der betroffenen Personen und die entsprechenden Pflichten der Verantwortlichen.

Den folgenden Fragen wird nachgegangen:

- Welche Informationen müssen den betroffenen Personen mitgeteilt werden?
- Welche Rechte haben betroffene Personen an ihren Daten?
- Wie lässt sich garantieren, dass die betroffenen Personen ihre Rechte geltend machen können?
- Wie lässt sich garantieren, dass das Verfahren zur Ausübung des Auskunftsrechts immer gleich abläuft (Reproduzierbarkeit des Verfahrens)?

3.1 INFORMATIONSPFLICHT

Die Artikel 19–21 DSG und Artikel 13 DSV betreffen die Informationspflicht und die Ausnahmen davon. Der Verantwortliche muss die betroffene Person angemessen über die Beschaffung von Personendaten informieren. Diese Informationspflicht gilt auch, wenn die Daten nicht direkt bei der betroffenen Person beschafft werden.

Die betroffene Person muss die Informationen erhalten, die erforderlich sind, damit sie gegebenenfalls ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Werden die Daten nicht bei der betroffenen Person beschafft, so muss sie spätestens einen Monat nach der Beschaffung oder – falls dies vorher erfolgt – zum Zeitpunkt der Bekanntgabe der Daten die Information erhalten.

Die Informationen umfassen mindestens:

- die Identität und die Kontaktdaten des Verantwortlichen;
- den Bearbeitungszweck;
- die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden;
- wenn die Daten nicht bei der betroffenen Person beschafft werden, die Kategorien der bearbeiteten Personendaten;
- wenn die Personendaten ins Ausland bekanntgegeben werden, den betreffenden Staat oder das betreffende internationale Organ und gegebenenfalls die getroffenen Massnahmen zur Gewährleistung eines angemessenen Schutzes (Art. 16 und 17 DSG).

Ausnahmen
Nach Artikel 20 Absätze 1 und 2 DSG entfällt die Informationspflicht bezüglich der Beschaffung von Personendaten, wenn eine der folgenden Voraussetzungen erfüllt ist:

- Die betroffene Person verfügt bereits über die entsprechenden Informationen.
- Die Bearbeitung ist gesetzlich vorgesehen.
- Es handelt sich beim Verantwortlichen um eine private Person, die gesetzlich zur Geheimhaltung verpflichtet ist.
- Die Personendaten werden nicht bei der betroffenen Person beschafft und die Information ist nicht möglich oder erfordert einen unverhältnismässigen Aufwand.

Medien können unter den Voraussetzungen nach Artikel 27 DSG ebenfalls auf eine Information verzichten.

Einschränkungen
Artikel 20 Absatz 3 und 27 DSG erlauben dem Verantwortlichen, die Mitteilung der Informationen in den folgenden Fällen einzuschränken, aufzuschieben oder darauf zu verzichten:

- Überwiegende Interessen Dritter erfordern die Massnahme.
- Die Information vereitelt den Zweck der Bearbeitung.
- Überwiegende Interessen des Verantwortlichen erfordern die Massnahme und er gibt die Personendaten nicht Dritten bekannt.

Beispiele für überwiegende Interessen Dritter wären hier zum Beispiel, um ihren Vertrag mit der betroffenen Person zu erfüllen oder die Sicherheit der Datenbearbeitung zu gewährleisten. Ein Beispiel für ein eigenes überwiegendes Interesse wäre, um Direktmarketing an die betroffene Person zu richten (ohne Weitergabe an Dritte).

Für Medien bestehen zusätzliche Möglichkeiten, die in Artikel 27 DSG präzisiert sind.

Automatisierte Einzelentscheidungen
Artikel 21 DSG verpflichtet den Verantwortlichen auch, die betroffene Person über eine Entscheidung zu informieren, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

Die betroffene Person muss auf Antrag ihren Standpunkt darlegen können. Ausserdem kann sie verlangen, dass eine natürliche Person den Entscheid überprüft.

Ausnahmen zu dieser Regel bestehen in zwei Fällen:

- wenn die automatisierte Entscheidung in unmittelbarem Zusammenhang mit einem Vertrag zwischen der betroffenen Person und dem Verantwortlichen steht und mit der Entscheidung ihrem Begehren stattgegeben wird;
- wenn die betroffene Person ausdrücklich einwilligt, dass die Entscheidung automatisiert erfolgt.

3.2 Rechte der betroffenen Personen

Neben dem Recht, informiert zu werden, haben die betroffenen Personen in Zusammenhang mit ihren Personendaten mehrere weitere Rechte. Diese sind in den Artikeln 25–29 sowie 32 DSG umschrieben. Konkret können diese Rechte im Rahmen eines Zivilverfahrens gestützt auf die Artikel 28 ff. des Zivilgesetzbuches oder das Vertragsrecht geltend gemacht werden.

Die Rechte, welche die betroffenen Personen gegenüber Bundesorganen geltend machen können, sind im Wesentlichen ähnlich wie die in diesem Kapitel beschriebenen; für weitergehende Informationen wird auf Abschnitt «Rechte der betroffenen Personen» verwiesen.

3.2.1 Auskunftsrecht

Nach Artikel 25 DSG kann jede Person vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Sie erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Diese Informationen umfassen mindestens:

- die Identität und die Kontaktdaten des Verantwortlichen;
- die bearbeiteten Personendaten;
- den Bearbeitungszweck;
- die Aufbewahrungsdauer der Personendaten oder, falls diese noch nicht bestimmt werden kann, die Kriterien zur Festlegung dieser Dauer;
- sofern die Daten nicht bei der betroffenen Person beschafft wurden, die verfügbaren Angaben über die Herkunft der Personendaten;
- gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;
- gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Artikel 19 Absatz 4 DSG.

Personendaten über die Gesundheit können der betroffenen Person mit ihrer Einwilligung durch eine von ihr bezeichnete Gesundheitsfachperson mitgeteilt werden (Art. 25 Abs. 3 DSG).

Die Auskunft muss innerhalb von 30 Tagen und grundsätzlich kostenlos erteilt werden. Wenn Daten von einem Auftragsbearbeiter bearbeitet werden, muss dieser den Verantwortlichen bei der Auskunftserteilung unterstützen. Die Modalitäten rund um das Auskunftsrecht sind in den Artikeln 16–19 DSV geregelt.

Einschränkungen

Artikel 26 DSG gibt dem Verantwortlichen die Möglichkeit, die Auskunft zu verweigern, einzuschränken oder aufzuschieben, wenn:

- ein Gesetz im formellen Sinn dies vorsieht, namentlich um ein Berufsgeheimnis zu schützen;
- dies aufgrund überwiegender Interessen Dritter erforderlich ist;
- das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist; oder
- überwiegende Interessen des Verantwortlichen die Massnahme erfordern und er die die Personendaten nicht Dritten bekanntgibt.

Der Verantwortliche muss innerhalb von 30 Tagen mitteilen, weshalb er die Auskunft verweigert, einschränkt oder aufschiebt.

Für Medien sind zusätzliche Ausnahmen möglich. Die Voraussetzungen sind in Artikel 27 DSG festgelegt.

Massnahmen:

- Es muss klar und verständlich informiert werden, damit jede und jeder die eigenen Rechte kennt und ausüben kann.
- Für Auskunftsgesuche ist ein Verfahren einzurichten und bei den Mitarbeitenden bekanntzumachen.
- Das System ist so organisiert, dass Auskunftsgesuche beantwortet werden können: Über die Suche müssen rasch sämtliche Daten der betroffenen Person gefunden werden können.
- Daten, zu denen die Auskunft eingeschränkt werden könnte, sind klar als solche gekennzeichnet und der Grund ist vermerkt.
- Im Falle einer Bearbeitung durch einen Auftragsbearbeiter muss auch definiert werden, nach welchem Verfahren dieser die Daten übermittelt.

3.2.2 Recht auf Datenherausgabe oder -übertragung

Nach Artikel 28 DSG kann eine betroffene Person vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen, wenn:

– der Verantwortliche die Daten automatisiert bearbeitet; und
– die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.

Unter den gleichen Voraussetzungen kann die betroffene Person zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen überträgt, wenn dies keinen unverhältnismässigen Aufwand erfordert.

Die Herausgabe und die Übertragung der Personendaten sind grundsätzlich kostenlos. Die möglichen Einschränkungen dieses Rechts entsprechen jenen beim Auskunftsrecht (Art. 29 DSG).

Die Einzelheiten, namentlich die technischen Anforderungen, in Zusammenhang mit der Ausübung dieses Rechts sind in den Artikeln 20–22 DSV beschrieben.

Die Europäische Union hat «Leitlinien zum Recht auf Datenübertragbarkeit»[10] veröffentlicht, die für die Umsetzung dieser Rechte als Grundlage dienen können.

Massnahmen:

- Bei der Konzeption einer automatisierten Datenbearbeitung ein gängiges Format verwenden, um die Datenextraktion zu erleichtern.
- Alternativ eine Methode zur Umwandlung der Personendaten in ein gängiges Format vorsehen.
- Abklären, ob Standards oder Vorlagen für die Übertragung spezifischer Arten von Personendaten (z. B. biometrische, genetische) existieren.
- Protokolle für die Herausgabe oder Übertragung von Personendaten erstellen und bei den Mitarbeitenden bekanntmachen.
- Die Machbarkeit des Imports von Personendaten aus Systemen anderer Verantwortlicher, die ähnliche Bearbeitungen vornehmen, prüfen.

[10] ARTICLE 29 – Guidelines on the right to «data portability» (wp242rev.01) (europa.eu)

3.2.3 Recht auf Vernichtung der Personendaten

Artikel 32 Absatz 2 Buchstabe c DSG sieht vor, dass die betroffene Person die Löschung oder die Vernichtung ihrer Personendaten verlangen kann. Dieses Recht, das durch Löschen oder Anonymisieren der Personendaten umgesetzt wird, kann bei umfangreichen Bearbeitungen komplex zu verwirklichen sein, dies angesichts des häufig internationalen Aspekts solcher Bearbeitungen und der Fortschritte der heutigen Technologie, beispielsweise der Verwendung der Cloud auf Servern auf mehreren Kontinenten.

Bei der Datenvernichtung muss das System garantieren, dass sämtliche von dem Begehren betroffenen Daten (was nicht unbedingt allen Personendaten der betroffenen Person entspricht) gelöscht/anonymisiert werden (Datenvernichtung). Dies ist wesentlich einfacher zu bewerkstelligen, wenn das System nach den Grundsätzen des Datenschutzes durch Technik (*Privacy by design)* und datenschutzfreundliche Voreinstellungen konzipiert wurde (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen).

3.2.4 Recht auf Berichtigung der Personendaten

Nach Artikel 32 Absatz 1 DSG können die betroffenen Personen verlangen, dass unrichtige Personendaten berichtigt werden, es sei denn, eine gesetzliche Vorschrift verbietet die Änderung oder die Personendaten werden zu Archivzwecken im öffentlichen Interesse bearbeitet.

Gegebenenfalls muss der Verantwortliche sich vergewissern, dass die Daten in allen seinen Systemen und Datenbanken angepasst werden. Auch muss er überprüfen, ob darauf basierend Entscheidungen ergangen sind. Je nach Fall könnte es relevant sein, zu kontrollieren, ob Entscheidungen auf diesen unrichtigen Daten basierten.

Kann weder die Richtigkeit noch die Unrichtigkeit der betreffenden Personendaten festgestellt werden, so kann die betroffene Person verlangen, dass ein Bestreitungsvermerk angebracht wird (Art. 32 Abs. 3 DSG).

Es ist zu empfehlen, sich auf solche Situationen vorzubereiten, indem klar definierte Prozesse festgelegt und geeignete Mittel bereitgestellt werden (namentlich Felder für den Bestreitungsvermerk vorsehen).

3.2.5 Recht auf Verbot der Bearbeitung von Personendaten

Nach Artikel 32 Absatz 2 Buchstabe a DSG kann die betroffene Person verlangen, dass die Bearbeitung ihrer Personendaten untersagt wird.

Nebst Situationen, in denen die Person eine Bearbeitung untersagen lassen möchte, weil sie sie insgesamt als nicht gerechtfertigt erachtet, ist dieses Recht auch in «Mischsituationen» sinnvoll, namentlich wenn Daten zu verschiedenen Zwecken bearbeitet werden. Ein Beispiel ist die Verwendung einer E-Mail-Adresse zur Registrierung eines Benutzerkontos sowie für den Versand des wöchentlichen Newsletters der Website. In diesem Fall kann die betroffene Person verlangen, dass ihre Adresse nicht mehr für den Newsletter-Versand benutzt wird.

Ein anderer Fall ist, wenn Personendaten von Gesetzes wegen aufbewahrt werden müssen (z. B. Patientendossiers), die betroffene Person aber wünscht, dass der Verantwortliche sie zu keinem anderen Zweck verwendet. In diesem Fall kann sie jegliche Bearbeitung, die über diesen Zweck hinausgeht, verbieten lassen.

Um solchen Begehren zu entsprechen, muss der Verantwortliche seine verschiedenen Bearbeitungen voneinander trennen können. Es ist daher empfohlen, einen einfachen Prozess vorzusehen, damit spezifische Bearbeitungen beendet werden können (z. B. Newsletter-Abmeldung, indem beim entsprechenden Kästchen das Häkchen entfernt wird).

3.2.6 Recht auf Verbot der Bekanntgabe von Personendaten

Nach Artikel 32 Absatz 2 Buchstabe b DSG kann die betroffene Person verlangen, dass eine bestimmte Bekanntgabe von Personendaten an Dritte untersagt wird.

Eine Möglichkeit, solchen Begehren zu entsprechen, ohne jedoch die Daten zu löschen, ist, ein Attribut betreffend die Einwilligung zur Bekanntgabe vorzusehen. Solche Massnahmen können mit jenen zur Einschränkung der Bearbeitungszwecke (siehe oben) gekoppelt werden.

3.2.7 Recht auf Mitteilung der Massnahmen betreffend Personendaten

Schliesslich kann die betroffene Person ausserdem verlangen, dass die unter 3.2.3 bis 3.2.6 beschriebenen Massnahmen veröffentlicht oder Dritten mitgeteilt werden (Art. 32 Abs. 4 DSG).

Massnahmen:

- Die Bearbeitungssysteme sind so organisiert, dass den verschiedenen Begehren entsprochen werden kann, ohne die Gesamtheit der Bearbeitungen zu gefährden.
- Es bestehen klare, vordefinierte Verfahren zur Beantwortung solcher Begehren; diese sind den Mitarbeitenden bekannt.
- Die Verfahren zur Ausübung der verschiedenen Rechte sind für die betroffenen Personen leicht zugänglich und einfach zu nutzen, beispielsweise in einem Bereich «Datenschutz» oder «Mein Konto».
- Sind Personendaten online, kann es sinnvoll sein, gewisse Seiten von der Suchmaschinenindexierung auszunehmen, um die Wahrung der Rechte betroffener Personen zu erleichtern.

3.3 REPRODUZIERBARKEIT DER VERFAHREN

Die Verfahren, mit denen Begehren von betroffenen Personen um Ausübung ihrer verschiedenen Rechte entsprochen wird, müssen klar festgelegt und reproduzierbar sein. Wenn die Mechanismen im Datenbearbeitungssystem vorprogrammiert sind, können alle Mitarbeitenden, die über die entsprechenden Berechtigungen verfügen, die verschiedenen von den betroffenen Personen verlangten Massnahmen an den Daten vornehmen. Ein vorprogrammierter Mechanismus ist auch praktisch bei einer Kontrolle durch eine Aufsichtsbehörde, weil er belegt, dass den Begehren der betroffenen Personen in Zusammenhang mit ihren verschiedenen Rechten auf Antrag entsprochen werden kann.

Massnahmen:

- Das Verfahren zur Ausübung des Auskunftsrechts ist im System vorprogrammiert.
- Alle Mitarbeitenden gehen nach dem gleichen Verfahren vor.
- Die Aufsichtsbehörde kann bei ihrer Arbeit wenn nötig das ins System integrierte Verfahren überprüfen.

Weitergehende Informationen:

	CNIL [6]
Ausübung des Rechts auf Einschränkung der Bearbeitung	Ziff. 11
Ausübung der Rechte auf Berichtigung und Löschung	Ziff. 12
Ausübung des Auskunftsrechts und des Rechts auf Übertragbarkeit (DSGVO)	Ziff. 13

Zwecke: bestimmt, explizit und rechtmässig	Ziff. 14
Grundlage: Rechtmässigkeit der Bearbeitung, Verbot der Zweckentfremdung	Ziff. 15
Vorherige Formalitäten	Ziff. 16
Information der betroffenen Personen	Ziff. 22
Einholung der Einwilligung	Ziff. 30

4 BUNDESORGANE

Im Grossen und Ganzen unterstehen die Bundesorgane denselben Regeln und Grundsätzen wie Private, abgesehen von gewissen Abweichungen. Die Artikel 33–42 DSG legen die spezifisch für Bundesorgane geltenden Regeln fest. Ebenso ist die Regelung in der DSV für Bundesorgane punktuell anders (etwa Art. 4 Abs. 2 oder Art. 6 DSV). Da sich dieser Leitfaden in erster Linie an Privatpersonen richtet, werden die Besonderheiten für Bundesorgane nur kurz skizziert. Weitergehende Informationen finden sich auf der Website des Bundesamts für Justiz[11].

4.1 GESETZLICHE GRUNDLAGEN

Grundsätzlich dürfen Bundesorgane Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 34 DSG).

Wenn die Bearbeitung besonders schützenswerte Personendaten oder Profilings betrifft oder zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen könnte, ist gar eine Grundlage in einem Gesetz im formellen Sinn erforderlich (Art. 34 Abs. 2 DSG).

Dennoch kann für die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling eine Grundlage in einem Gesetz im materiellen Sinn ausreichend sein, wenn der Bearbeitungszweck für die Grundrechte der betroffenen Person keine besonderen Risiken birgt und die Bearbeitung für eine Aufgabe, die ihrerseits in einem Gesetz im formellen Sinn festgelegt ist, unentbehrlich ist (Art. 34 Abs. 3 DSG).

Schliesslich dürfen Bundesorgane in Abweichung von den vorangehenden Ausführungen Personendaten bearbeiten, wenn eine der drei folgenden Voraussetzungen erfüllt ist (Art. 34 Abs. 4 DSG):

- Der Bundesrat hat die Bearbeitung bewilligt, weil er die Rechte der betroffenen Person für nicht gefährdet hält.
- Die betroffene Person hat im Einzelfall in die Bearbeitung eingewilligt oder hat ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt.
- Die Bearbeitung ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.

4.2 DATENBEARBEITUNG FÜR NICHT PERSONENBEZOGENE ZWECKE

Nach Artikel 39 DSG dürfen Bundesorgane Personendaten für Forschungs-, Planungs- oder Statistikzwecke bearbeiten, wenn:

- die Daten anonymisiert werden, sobald der Bearbeitungszweck dies erlaubt;
- das Bundesorgan privaten Personen besonders schützenswerte Personendaten nur so bekanntgibt, dass die betroffenen Personen nicht bestimmbar sind;
- die Empfängerin oder der Empfänger Dritten die Daten nur mit der Zustimmung des Bundesorgans weitergibt, das die Daten bekanntgegeben hat; und
- die Ergebnisse nur so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

[11] Informationen für Bundesorgane (admin.ch)

Diese Bestimmung begründet eine Ausnahme vom Prinzip der Zweckbindung und stellt zudem eine Lockerung der Anforderungen bezüglich der erforderlichen Gesetzesgrundlage für die Bearbeitung und Bekanntgabe von Daten dar (vgl. Art. 39 Abs. 2 und die dort zitierten Artikel).

4.3 Bekanntgabe

Insgesamt unterliegt die Bekanntgabe von Personendaten den gleichen Voraussetzungen wie die Bearbeitung selbst (vgl. Art. 36 Abs. 1, der auf Art. 34 Abs. 1–3 DSG verweist; siehe auch weiter oben). In Artikel 36 Absatz 2 DSG sind jedoch spezifische Abweichungsmöglichkeiten vorgesehen: Dabei handelt es sich vor allem um Situationen, in denen dies zur Erfüllung einer Aufgabe unentbehrlich ist, oder wenn es übergeordnete Interessen zu schützen gilt oder aber wenn sich die Person entgegen Treu und Glauben gegen die Bekanntgabe wehrt. Ein weiterer Rechtfertigungsgrund für eine Bekanntgabe ist die Einwilligung der betroffenen Person.

Generell dürfen Bundesorgane auch Name, Vorname, Adresse und Geburtsdatum einer Person auf Anfrage bekanntgeben (Art. 36 Abs. 4 DSG). Dabei handelt es sich jedoch um ein Recht und nicht eine Pflicht: Das Bundesorgan muss immer eine Interessenabwägung aus Sicht der Datenschutzgrundsätze vornehmen. Die Bundesorgane dürfen zudem in den Fällen nach Artikel 36 Absätze 3 und 5 DSG Daten der Öffentlichkeit bekanntgeben oder allgemein zugänglich machen.

Schliesslich können Bundesorgane die Bekanntgabe generell ablehnen, wenn sie an gesetzliche Geheimhaltungspflichten gebunden sind oder ein wesentliches öffentliches oder privates Interesse besteht (Art. 36 Abs. 6 DSG). Zu beachten ist zudem, dass die betroffene Person auch Widerspruch gegen die Bekanntgabe von Personendaten einlegen kann; über das Begehren entscheidet das Bundesorgan (Art. 37 DSG).

4.4 Verzeichnis der Datenbearbeitungen

Die Bundesorgane müssen ein Verzeichnis der Bearbeitungstätigkeiten führen, das vom Inhalt her ähnlich ist wie jenes Verzeichnis, das Privatpersonen führen müssen (Art. 12 DSG, vgl. Verzeichnis). Sie müssen ihre Verzeichnisse ausserdem dem EDÖB melden (Art. 12 Abs. 4 DSG). Dies können sie über das entsprechende Meldeportal tun.[12]

4.5 Meldung von Verletzungen der Datensicherheit

Die Bundesorgane unterstehen derselben Meldepflicht für Verletzungen der Datensicherheit wie Private (Art. 24 DSG). Ein kleiner Unterschied besteht allerdings bei den Gründen, aus denen sie die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten können: Hier ist nicht das Interesse Dritter ausschlaggebend, sondern die Wahrung überwiegender öffentlicher Interessen oder die Nichtgefährdung einer Ermittlung, Untersuchung oder eines Verfahrens (Art. 24 Abs. 5 Bst. a, der auf Art. 26 Abs. 2 Bst. b DSG verweist).

4.6 Automatisierte Einzelentscheidungen

Im Grossen und Ganzen ist die Regelung im Bereich automatisierter Einzelentscheidungen für Bundesorgane dieselbe wie für Privatpersonen. Zu beachten sind aber zwei Unterschiede, die in Artikel 21 Absatz 4 DSG festgelegt sind:

1) Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen.

[12] Datareg: http://datareg.edoeb.admin.ch/

2) Die betroffene Person hat keine Möglichkeit, ihren Standpunkt darzulegen, und kann nicht verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird, wenn die betroffene Person auf der Grundlage eines Bundesgesetzes (z. B. Art. 30 Abs. 2 VwVG) vor dem Entscheid nicht angehört werden muss.

4.7 INFORMATIONSPFLICHT

Auch hier untersteht ein Bundesorgan im Wesentlichen den gleichen Regeln wie eine Privatperson (Informationspflicht). Im Unterschied zu einer Privatperson kann ein Bundesorgan allerdings die Information nicht aufgrund eigener Interessen einschränken, aufschieben oder darauf verzichten (Art. 20 Abs. 3 Bst. c DSG), sondern aufgrund öffentlicher Interessen oder um eine Ermittlung, eine Untersuchung oder ein Verfahren nicht zu gefährden (Art. 20 Abs. 3 Bst. d DSG).

4.8 RECHTE DER BETROFFENEN PERSONEN

Generell müssen Bundesorgane in Bezug auf die Rechte betroffener Personen denselben Anforderungen genügen wie Privatpersonen (Rechte und Pflichten).

Ein Bundesorgan kann allerdings nicht aufgrund eigener Interessen die Auskunft verweigern, einschränken oder aufschieben. Es kann dies aber aufgrund öffentlicher Interessen oder um eine Ermittlung, eine Untersuchung oder ein Verfahren nicht zu gefährden (Art. 26 Abs. 2 Bst. b DSG).

Hinsichtlich der Ausübung ihrer Rechte verfügt die betroffene Person materiell mehr oder weniger über die gleichen Ansprüche wie gegenüber Privatpersonen (Art. 41 gegenüber Art. 32 DSG). Artikel 41 DSG regelt gewisse Nuancen in der Art oder Umsetzung dieser Ansprüche. Zu beachten ist insbesondere, dass sich ein solches Verfahren nach dem VwVG richten würde (Art. 41 Abs. 6 DSG).

Schliesslich regelt Artikel 42 DSG die Koordination zwischen Verfahren nach dem Öffentlichkeitsgesetz und den Rechten nach Artikel 41 DSG.

Massnahmen:

- Die gesetzliche Grundlage und/oder den Grund für die Datenbearbeitung immer klar angeben.
- Die Personendaten kennzeichnen, für die Ausnahmen bezüglich der verschiedenen Rechte betroffener Personen gelten.
- Ähnliche Verfahren vorbereiten, wie im Abschnitt Rechte und Pflichten empfohlen.

4.9 PROTOKOLLIERUNG

Bundesorgane und ihre Auftragsbearbeiter müssen in jedem Fall eine Protokollierung sicherstellen, wenn sie Personendaten automatisiert bearbeiten. Protokolliert werden muss mindestens das Speichern, Ändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten.

Überdies sind auch die Anforderungen hinsichtlich der Protokollierung durch private Verantwortliche anwendbar (Protokollierung).

4.10 BEARBEITUNGSREGLEMENT

Bei bestimmten Arten von automatisierten Bearbeitungen (vgl. Art. 6 Abs. 1 DSV) sind die Bundesorgane verpflichtet, ein Bearbeitungsreglement zu erstellen. Der Inhalt entspricht dem,

was für Reglemente von Privatpersonen verlangt wird (Bearbeitungsreglement). Der EDÖB stellt den Bundesorganen zu diesem Thema ein Hilfsdokument zur Verfügung[13].

[13] Bearbeitungsreglement (Bundesorgane) (DOCX)

5 DATENSCHUTZ

Der Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, den Artikel 7 DSG und Artikel 25 DSGVO vorgeben, umfasst Massnahmen zur Minimierung der Beschaffung von Personendaten wie auch ihrer Zugänglichkeit.

Der Grundsatz der Verhältnismässigkeit nach Artikel 6 Absatz 2 DSG und Artikel 5 Absatz 1 Buchstabe c DSGVO beinhaltet namentlich die Begrenzung des Zugriffs auf Personendaten.

Der Grundsatz der Datenrichtigkeit ist in Artikel 6 Absatz 5 DSG und Artikel 5 Absatz 1 Buchstabe d DSGVO verankert.

Dieser Abschnitt legt Massnahmen dar, mit denen der Inhalt der Personendaten geschützt wird. Die beschriebenen Techniken und Vorgehensweisen zur Verbesserung des Datenschutzes werden direkt auf inhaltlicher Ebene umgesetzt.

Artikel 7 Absätze 1 und 2 DSG nennt ausdrücklich die Pflicht des Verantwortlichen, ab der Planung die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. Beispielsweise erlauben die Verschlüsselung (Verschlüsselung von Mitteilungen) oder Pseudonymisierung (Pseudonymisierung) in gewissen Phasen der Bearbeitung einen besseren Schutz der Personendaten der betroffenen Personen.

In diese Kategorie gehören (technische) Massnahmen, die bei den Dateninhalten ansetzen. Diese sollen weniger genau, weniger sensibel gemacht werden, indem sie den angestrebten Zwecken gemäss angepasst werden. Ziel ist, die in den Daten enthaltene Information anzupassen (zu minimieren). Anders gesagt: Während die Datenmenge gleich bleibt (z. B. ID, Geschlecht, genaue Adresse), wird je nach Bearbeitungszweck unterschieden, welche Informationen ausgegeben werden (z. B. ID, Geschlecht, Kanton).

Dieses Anpassen der Information dient auch:

- deren Anpassung an den vorgesehenen Bearbeitungszweck (Grundsatz der Verhältnismässigkeit);
- der Informationssicherung (Grundsatz der Sicherheit) – gelangen die Daten in falsche Hände, ist die einsehbare Information weniger genau und weniger sensibel;
- allenfalls der Anonymisierung der Daten.

5.1 DATENSCHUTZ DURCH TECHNIK UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Der Datenschutz durch Technik (Art. 7 Abs. 1 DSG) erfordert, dass der Verantwortliche die Grundsätze des Datenschutzes ab der Planung des Systems mitberücksichtigt – und nicht erst später. Werden bereits vor der Realisierung der Bearbeitung Überlegungen zur Rechtfertigung der Datenbeschaffung sowie zur Verwendung, Verwaltung und Organisation der Daten angestellt, kann sichergestellt werden, dass die Datenschutzbestimmungen eingehalten und die Empfehlungen dieses Leitfadens umgesetzt werden.

Die datenschutzfreundlichen Voreinstellungen (Art. 7 Abs. 3 DSG) sind ein Ausdruck des Grundsatzes der Verhältnismässigkeit. Hierbei geht es darum, dass der Verantwortliche ab dem Moment der Datenbeschaffung Massnahmen ergreift, die sicherstellen, dass von vornherein, namentlich durch Voreinstellungen, nur die für den Bearbeitungszweck strikt notwendige

Datenmenge beschafft und verwendet wird. Beispielsweise sollten bei der Sammlung von Cookies auf einer Website diejenigen, die für die Abfrage der Website nicht notwendig sind, standardmässig deaktiviert sein, sodass Nutzerinnen und Nutzer, welche mit der Verwendung zusätzlicher Cookies einverstanden sind, dieser aktiv zustimmen müssen.

Dieses Konzept gilt auch für sämtliche nachfolgenden Schritte der Bearbeitung: Der Verantwortliche muss dafür sorgen, dass jeder Bearbeitungsschritt mit dem absoluten Minimum an benötigten Informationen durchgeführt werden kann.

Die verschiedenen Massnahmen, die im Rahmen des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen umgesetzt werden, sind in der Regel in einer DSFA detailliert beschrieben (Datenschutz-Folgenabschätzung).

Massnahmen:

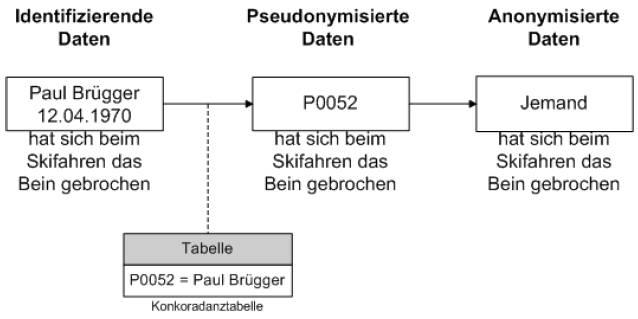
- Wenn auch für die Bearbeitung nicht notwendige Daten gesammelt werden, einen Wert vorsehen, der auf null oder negativ voreingestellt ist (z. B. «NA»).
- Für die Bearbeitung notwendige und nicht notwendige Daten klar kennzeichnen und trennen.
- Die Folgen der nicht zwingenden Informationen für die Effizienz der Anonymisierung und der Pseudonymisierung berücksichtigen.

5.2 PSEUDONYMISIERUNG

Im rechtlichen Sinne besteht die Pseudonymisierung darin, Personendaten so abzuändern, dass ohne zusätzliche Informationen oder unverhältnismässigen Aufwand kein Rückschluss mehr auf eine spezifische Person möglich ist. Bei pseudonymisierten Daten besteht aber nach wie vor das Risiko einer Re-Identifikation; sie gelten daher weiterhin als Personendaten.

Pseudonymisieren heisst, ein Pseudonym zu erstellen, dass typischerweise den Namen, das Geburtsdatum usw. der betroffenen Person in den Datenbanken ersetzt. Zugleich wird eine separate Konkordanztabelle erstellt, in welcher der Name mit dem Pseudonym verknüpft ist. So können nur Personen mit Zugriff auf diese Tabelle ohne Weiteres die Daten mit dem Namen verbinden und die Pseudonymisierung rückgängig machen.

Folgende Abbildung stellt diesen Prozess dar:



Es gibt verschiedene Möglichkeiten, um identifizierende Daten und Pseudonyme zuzuordnen, namentlich:

– die Erstellung von Konkordanztabellen, wie im Beispiel der Abbildung oben;
– die Nutzung von «Funktionen», bei denen identifizierende Daten eingegeben und die zugehörigen Pseudonyme ausgegeben werden.

Die Zuordnung – ob sie über eine Tabelle oder eine Funktion erfolgt – darf dabei nicht rückgängig gemacht werden können (ohne Beizug der Tabelle beispielsweise). Im Beispiel oben darf es nicht möglich sein, ohne Konsultation der Konkordanztabelle von P0052 auf «Paul Brügger» zu schliessen. Um dies zu gewährleisten, ist Folgendes zu beachten:

– Die Zuordnungen in der Konkordanztabelle müssen zufällig erstellt werden oder auf einem «Geheimnis» beruhen, das die Personen, welche die pseudonymisierten Daten verwenden, nicht kennen.
– Werden «Funktionen» verwendet, dürfen diese nicht umkehrbar sein, wie im Fall von kryptografischen Hash-Funktionen (SHA256, MD5 usw.). So wird SHA256(«Paul Brügger») etwa zu «671fee34b2bd82aec7bd60d757ebf3fd8f395d61b1dd70279d416e18b20937e1». Anhand dieses Outputs den Input zu erraten, ist praktisch unmöglich.
– Da die Hash-Funktionen öffentlich sind, ist es aber für die Person, welche die Pseudonyme verwendet, ein Leichtes, herauszufinden, was SHA256(«Paul Brügger») ergibt (oder auch eine ganze Namensliste, wie zum Beispiel die Liste der Namen aller Arbeitskolleginnen und -kollegen), um so «Paul Brügger» seinem Pseudonym «671…7e1» zuzuordnen. Um dies zu verhindern, ist zusammen mit den identifizierenden Daten ein geheimer Schlüssel zu verwenden, bevor die Hash-Funktion angewendet wird. So ergibt in unserem Beispiel SHA256(«Paul Brügger», «TopSecret») ein Pseudonym, das für die Benutzerinnen und Benutzer nicht umkehrbar ist, solange sie keinen Zugang zum geheimen Schlüssel («TopSecret») haben. Dies nennt sich schlüsselabhängige Hash-Funktion.
– Werden die Konkordanztabelle oder der geheime Schlüssel für das Hash-Verfahren vernichtet, sind Rückschlüsse vom Pseudonym auf die entsprechenden identifizierenden Daten nicht mehr möglich, und zwar weder für die Person, welche die Pseudonyme verwendet, noch für jene, welche die Konkordanztabelle oder das Hash-Verfahren erstellt hat. Durch das Vernichten der Verknüpfungen werden die Daten allerdings noch nicht anonym, wie im Folgenden ausgeführt wird.

5.3 ANONYMISIERUNG

Im rechtlichen Sinne besteht die Anonymisierung darin, Personendaten unumkehrbar so zu verändern, dass sie ohne unverhältnismässigen Aufwand nicht mehr Rückschlüsse auf eine konkrete Person zulassen[14]. Anonymisierte Daten gelten nicht mehr als Personendaten und fallen daher auch nicht mehr unter den Geltungsbereich des DSG.

Um die Anonymität der Daten sicherzustellen, reicht es häufig nicht, eine Tabelle mit identifizierenden Zeichenfolgen, die zur Unkenntlichmachung des Namens verwendet wurden, zu löschen. In einer Patientenliste eines Spitals beispielsweise erfüllt [ID 8128136, Frau, 42 Jahre, wohnhaft in (kleines Dorf), Behandlung wegen AIDS, Operationsdatum 12.07.2021] die Anonymitätsvoraussetzungen nicht. Selbst ohne den Namen, der dank der ID unkenntlich ist, wäre es beispielsweise für den Arbeitgeber der Person oder jemanden, der das Alter der Frau kennt und weiss, in welchem Dorf sie wohnt, nicht schwer herauszufinden, um wen es

[14] Darunter ist Folgendes zu verstehen: *«Ist der Aufwand für die Bestimmung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird […], liegt keine Bestimmbarkeit vor. Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Ob der Einsatz dieser Mittel vernünftig ist, muss mit Blick auf die Umstände, etwa den zeitlichen und finanziellen Aufwand für die Identifizierung, beurteilt werden. Dabei sind die zum Zeitpunkt der Bearbeitung verfügbaren Technologien und deren Weiterentwicklung zu berücksichtigen.»* (Botschaft zum DSG, BBl 2017 S. 7019).

sich handelt. Je kleiner die Anzahl betroffener Personen und je mehr weitere Daten vorhanden sind, desto einfacher ist es, die Person wieder zu identifizieren.

Es gibt verschiedene Anonymisierungstechniken, die im Folgenden beschrieben werden. Allerdings sind diese nicht immer ausreichend, um alle Datensätze zu anonymisieren. Jeder neue Datensatz muss im Einzelfall betrachtet werden, und gewisse Datensätze können schlicht und einfach nicht anonymisiert werden, ohne dass sie ihren Nutzen verlieren (wodurch der Verantwortliche nur noch die Wahl hat, entweder Personendaten zu bearbeiten oder ganz auf die Bearbeitung zu verzichten). Darüber hinaus erfordern gewisse Datentypen andere Techniken. Beispielsweise braucht es spezielle Techniken für die Anonymisierung von Personen in Videos oder Fotografien.

Um den Anonymisierungsgrad über die juristische Definition hinaus einschätzen zu können, gibt es verschiedene Risikomodelle. Gemäss der Definition aus der Stellungnahme zu Anonymisierungstechniken [7] der Artikel-29-Datenschutzgruppe[15] sind die Risiken:

- *Herausgreifen (singling out),* d. h. die Möglichkeit, in einem Datenbestand einige oder alle Datensätze zu isolieren, welche die Identifizierung einer Person ermöglichen;
- *Verknüpfbarkeit,* d. h. die Fähigkeit, mindestens zwei Datensätze, welche dieselbe Person oder Personengruppe betreffen, zu verknüpfen (in derselben Datenbank oder in zwei verschiedenen Datenbanken). Ist ein Angreifer in der Lage (z. B. mittels Korrelationsanalyse) festzustellen, dass zwei Datensätze dieselbe Personengruppe betreffen, ohne jedoch einzelne Personen in dieser Gruppe herauszugreifen, bietet die betreffende Technik zwar einen Schutz vor dem «Herausgreifen», nicht aber vor der Verknüpfbarkeit;
- *Inferenz,* d. h. die Möglichkeit, den Wert eines Merkmals mit einer signifikanten Wahrscheinlichkeit von den Werten einer Reihe anderer Merkmale abzuleiten.

Eine Lösung, die Schutz vor diesen drei Risiken bietet, wäre somit robust und geeignet, eine Reidentifizierung mit den Mitteln, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten, zu verhindern.

Dabei ist zu erwähnen, dass es zunehmend schwieriger wird, von einer echten (im technischen Sinne), absolut irreversiblen Anonymisierung zu sprechen. Die Gründe dafür sind:

- das Wachstum der Datenvolumen, die für eine Re-Identifizierung verwendet werden können;
- die immer einfacher werdende Zugänglichkeit dieser Daten;
- neue, leistungsstärkere und präzisere Algorithmen, die für die Re-Identifizierung verwendet werden können;
- Fortschritte im Bereich der Kryptografie, welche die bestehenden Techniken schwächen könnten.

[15] Inzwischen *European Data Protection Board* (EDPB).

Bewährte Anonymisierungsverfahren der Artikel-29-Gruppe[15]

Grundsätzlich:

– Der für die Verarbeitung Verantwortliche darf niemals nach dem Prinzip «Freigeben und Vergessen» handeln. Aufgrund des Restrisikos der Identifizierung sollte er:

    1. regelmässig neue Risiken ermitteln und die Restrisiken erneut evaluieren;
    2. prüfen, ob die Kontrollmechanismen für die ermittelten Risiken ausreichen, und diese gegebenenfalls entsprechend anpassen;
    3. die Risiken überwachen und steuern.

– Im Rahmen der Bewertung dieser Restrisiken ist (gegebenenfalls) auch das Identifizierungspotenzial des nicht anonymisierten Teils des Datenbestands zu berücksichtigen, wobei insbesondere die Möglichkeit seiner Kombination mit dem anonymisierten Teil des Datenbestands sowie potenzielle Korrelationen zwischen Merkmalen (z. B. zwischen Daten über Standort und Wohlstandsniveau) in Betracht zu ziehen sind.

Massnahmen:

- Im Rahmen der Möglichkeiten die Verwendung von anonymisierten Daten vorziehen. Wenn die Daten korrekt anonymisiert sind, ist das Datenschutzgesetz nicht mehr anwendbar.
- Im Falle der Anonymisierung wird keine indirekt identifizierende Information aufbewahrt. Eine indirekt identifizierende Information ist eine Information, die zusammen mit anderen Informationen, die für sich allein keine Bedeutung haben, die Identifikation einer Person erlauben.
- Wenn eine Anonymisierung nicht in Betracht kommt, arbeiten die Mitarbeitenden wenn möglich mit pseudonymisierten Daten.
- Die Konkordanztabelle und/oder der geheime Schlüssel des Hash-Verfahrens müssen gesichert werden. Sie dürfen nur einer beschränkten Anzahl Mitarbeitenden zugänglich und sollten wenn möglich verschlüsselt sein.

5.4 GENERALISIERUNG

Die Generalisierung besteht darin, gewisse Merkmalswerte durch allgemeinere Werte oder Wertebandbreiten zu ersetzen. Zum Beispiel:

- ein Geburtsdatum (z. B. 8.3.1980) durch das Geburtsjahr (z. B. 1980) oder eine Altersspanne (z. B. [40–50] Jahre);
- eine genaue Adresse durch die Stadt, die Region oder den Kanton (sehr gut hierarchisch abstufbar);
- eine Nationalität durch die geografische Region oder den Kontinenten.

Durch die Generalisierung sind die Merkmale weniger nützlich für die Re-Identifikation von Personen. Zum Beispiel:

– [Geschlecht: Frau, Alter: 32, Nationalität: Moldawierin, Wohnort: Morges] ist leicht identifizierbar. Eine generalisierte Form wie [Geschlecht: Frau, Alter: 30–40, Nationalität: Osteuropa, Wohnort: Region Lausanne] erschwert die Identifikation.
– Für einen Wetterdienst ist keine GPS-Granularität (~2 m) nötig. Durch deren Verwendung könnten Nutzerinnen und Nutzer unnötig identifiziert werden. Eine Generalisierung auf Stufe Ortschaft ist eher angebracht.

Die Datengeneralisierung trägt bei zur:

- allfälligen Anonymisierung der Daten (die somit nicht mehr unter das DSG und die DSGVO fallen);
- Verhältnismässigkeit der beschafften Information, unabhängig davon, ob die Daten anonym sind;
- Datensicherung, unabhängig davon, ob die Daten anonym sind.

5.5 MINIMIERUNG

Die Minimierung ist eine konkrete Anwendung des Datenschutzes durch Technik und besteht darin, nur das absolute Minimum an notwendigen Daten zu beschaffen. Denn gewisse Daten oder deren Kombination können zur Identifizierung der betroffenen Personen beitragen, selbst wenn sie für sich allein genommen nicht personenbezogen oder besonders schützenswert sind.

Beispiele:

- Um die Transportmittel der Nutzerinnen und Nutzer einer bestimmten Applikation zu analysieren, kann deren Identität durch den Ausschluss der GPS-Daten rund um ihren jeweiligen Wohnort besser geschützt werden.
- Eine Applikation, die in einem bestimmten Land bestimmte Dienste (z. B. ÖV) während definierter Öffnungszeiten anbietet, sollte in anderen Ländern oder ausserhalb der Dienstzeiten die Lokalisierung der Nutzerinnen und Nutzer nicht erfassen.

Wie bei der Generalisierung trägt die Datenfilterung bei zur:

- Verhältnismässigkeit, unabhängig davon, ob die Daten anonym sind;
- Datensicherung, unabhängig davon, ob die Daten anonym sind.

5.6 RANDOMISIERUNG

Für gewisse Bearbeitungszwecke werden Daten beschafft, die statistische, nicht individuelle Ergebnisse liefern sollen. Dieser Fall ist ein typischer Einsatzbereich für die Randomisierung, das heisst, die zufällige Veränderung von Merkmalswerten. Will man zum Beispiel das Durchschnittsalter einer gewissen Population in Erfahrung bringen, so kann man die beschafften Einzelwerte ändern und behält dabei (fast) den gleichen ursprünglichen Durchschnitt.

Die Kategorie umfasst verschiedene Techniken, darunter namentlich:

- die stochastische Überlagerung, d. h. die Veränderung von Informationskategorien ohne Veränderung der für die Messung relevanten Informationen (z. B. bei einer Person fünf Jahre zum Alter hinzufügen und bei einer andern abziehen);
- die Vertauschung, d. h. die Verschiebung von Daten zwischen Datensätzen ohne Veränderung der für die Messung relevanten Informationen (z. B. das Alter zweier Personen vertauschen);
- die *Differential Privacy,* eine spezifische Randomisierungstechnik, welche die Stärke der Überlagerung bestimmt, die bei der Datenübermittlung anstatt direkt bei den Daten hinzuzufügen ist.

Zu beachten ist: Die Randomisierung ändert die Merkmalswerte, ohne aber die betroffenen Personen zu anonymisieren. Beispielsweise könnten Vor- und Nachnamen der Personen kenntlich bleiben, aber die Altersangaben stimmen nicht – und wären für sich allein genommen

unbrauchbar. Es handelt sich damit um eine Möglichkeit, die Risiken zu reduzieren, ohne die identifizierenden Daten zu verändern.

Liegen hingegen keine anderen identifizierenden Daten vor, tragen die randomisierten Merkmale indirekt zur Anonymisierung bei. Wird beispielsweise bei der Altersangabe eine stochastische Überlagerung vorgenommen, so ist im Fall von [Mann, 39 Jahre, Murten], wobei 39 = 34 + Überlagerung, die Identität der Person weniger klar.

5.7 Homomorphe Verschlüsselung

Bei der homomorphen Verschlüsselung verschlüsselt ein Algorithmus die Daten so, dass ihre mathematischen Eigenschaften erhalten bleiben. Dadurch können auch bei ausschliesslichem Zugang zur verschlüsselten Version bestimmte Informationen aus diesen Daten gemessen werden.

Von den machbaren Operationen her ist diese relativ neue Methode eingeschränkt, und sie kann sich in der Umsetzung als relativ kostspielig erweisen. Auf der anderen Seite kann sie die Bearbeitung von besonders schützenswerten Personendaten durch Dritte ermöglichen, ohne Gefahr eines Zugriffs durch diesen.

Es gibt auch sogenannt teilhomomorphe Algorithmen, mit denen in der Regel nur eine einzige Operation möglich ist. Dafür sind sie kostengünstiger.

5.8 Synthetische Daten

Synthetische Daten sind Daten, die ab echten Daten künstlich erzeugt werden, zum Beispiel mit einem *Machine-Learning*-Algorithmus. Diese Daten sind echten Personendaten genügend ähnlich, um andere Modelle darauf trainieren zu können (z. B. falsche Tumorbilder für ein medizinisches System).

Durch die Verwendung solcher Daten ist es grundsätzlich möglich, den Geltungsbereich des DSG zu verlassen, allerdings ist beim Datenerzeugungsprozess grosse Vorsicht geboten. Es darf nicht möglich sein, die Originaldaten wiederherzustellen oder die betroffenen Personen in den Original-Personendaten zu re-identifizieren (vgl. Anonymisierung). Solange dies nicht garantiert ist, müssen diese Daten gleichwohl als Personendaten betrachtet werden.

6 INFRASTRUKTUR

Die Datensicherheit, im Sinne von Artikel 8 DSG, Artikel 3 DSV sowie Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO, umfasst unter anderem auch die Sicherung der Räumlichkeiten, der Server und der Büros.

Die bislang beschriebenen Massnahmen konzentrieren sich auf den Dateninhalt. Ein weiterer Aspekt ist jedoch die Datenumgebung, namentlich die Infrastruktur und das Verhalten der Personen, welche die Daten bearbeiten. Der Ort, an dem die Daten physisch aufbewahrt werden, muss sorgfältig geprüft werden: Wo befinden sich die Datenserver, und wie kann ihre Sicherheit unter Berücksichtigung aller involvierten Akteure gewährleistet werden?

Zu den folgenden Aspekten finden sich in diesem Abschnitt detaillierte Informationen und konkrete Massnahmen:

- Wie werden die Räumlichkeiten gesichert?
- Wie wird der Schutz der Server sichergestellt?
- Wie wird der Schutz der Arbeitsplätze sichergestellt?
- Welche Risiken birgt die Auslagerung der Daten, beispielsweise durch Cloud-Nutzung?

6.1 SICHERHEIT DER RÄUMLICHKEITEN

Als Räumlichkeiten gelten die Büros derjenigen Personen, die das System benutzen und somit auch Zugang zu den Daten haben. Die Daten werden physisch in Serverräumen aufbewahrt (siehe nachfolgenden Abschnitt). Die PC sind die peripheren Geräte, über die auf die Daten zugegriffen werden kann. Daher muss der Zugang zu diesen Geräten kontrolliert werden. Nur berechtigte Personen dürfen also das Gebäude oder die Büros betreten. Diese Personen können jedoch ganz unterschiedliche Funktionen wahrnehmen, die bei der Ableitung spezifischer Zugangsberechtigungen zu berücksichtigen sind: Die Mitarbeitenden gehören selbstverständlich dazu, aber auch das Unterhalts- und das Reinigungspersonal usw.

Damit die geeigneten Massnahmen getroffen werden können, muss der ganze Kontext betrachtet werden. Befinden sich etwa mehrere Organisationen im selben Gebäude, haben nicht zwingend alle die gleichen Datenschutzbedürfnisse. Die Sicherheitsvorkehrungen müssen also zum Beispiel etagenweise angepasst werden. Zudem können die Server ausgelagert werden, womit andere für die räumliche Sicherheit zuständig sind.

Massnahmen:

- Der Zugang zum Gebäude wird geregelt. Dank einem Badge und allenfalls einem Zugangscode können die Personen, die zugangsberechtigt sind, authentifiziert werden.
- Eine ähnliche Regelung wird nötig, wenn sich mehrere Organisationen im selben Gebäude befinden: Auf jeder Etage oder für jeden Gebäudeteil, der für eine bestimmte Organisation vorgesehen ist, wird eine elektronische Zugangskontrolle installiert.
- Für Besucherinnen und Besucher werden Zugang und Empfang so geregelt, dass sie sich nicht allein und frei im Gebäude bewegen können.
- Die Büros werden ausserhalb der Arbeitszeiten abgeschlossen.
- Es ist ratsam, in den heikelsten Räumen ein Alarmsystem zu installieren, das ausserhalb der Arbeitszeiten aktiviert wird.

6.2 SICHERHEIT DER SERVERRÄUME

Die Serverräume sind in einer Organisation die anfälligsten Räume, da hier die Daten physisch lagern. Nur wenn geeignete Massnahmen den definitiven Verlust der Daten verunmöglichen, können deren Integrität und Verfügbarkeit garantiert werden. Auch hier ist festzulegen, wer Zutritt zu diesen Räumen haben soll. Je weniger Personen zutrittsberechtigt sind, desto besser die Sicherheit. Absichtliche oder unabsichtliche Manipulationen am Server, die zur Vernichtung oder Veränderung der Daten führen könnten, müssen verhindert werden. Deshalb sind zur Sicherung der Serverräume besondere Massnahmen zu treffen.

Massnahmen:

- So wenig Personen wie nötig erhalten die Zugangsberechtigung zum Serverraum. Die Anzahl Technikerinnen und Techniker, die zur Wartung der Server Zutritt zum Serverraum haben, ist zu beschränken. Es ist zudem sinnvoll, immer die gleichen vertrauenswürdigen Personen mit der Reinigung dieses Raumes zu betrauen.
- Der Zutritt zu den Serverräumen wird protokolliert.
- Um jeglichen unbefugten Zutritt zu vermeiden, wird ein Alarmsystem installiert, das ständig in Betrieb ist.
- Das Alarmsystem sollte auch automatisch auf Naturereignisse wie Feuer oder Überschwemmung reagieren.
- Idealerweise sollte sich der Serverraum im Keller befinden, weil dieser normalerweise weniger Türen und Fenster aufweist.

6.3 SICHERHEIT DER ARBEITSPLÄTZE

Die Mitarbeitenden bearbeiten die Daten auf ihren PC von ihrem Arbeitsplatz aus. Diese Arbeitsumgebung muss geschützt werden, was die strategische Anordnung der verschiedenen peripheren Geräte (Bildschirm, Drucker etc.) beinhaltet. Den Mitarbeitenden ist genügend abschliessbarer Stauraum zur Verfügung zu stellen.

Der PC ist mindestens mit einem sicheren Passwort zu schützen, das nur die betreffende Mitarbeiterin oder der betreffende Mitarbeiter kennt. Zudem muss er mit der nötigen Software gegen unbefugten Zugriff geschützt werden. Dieser Schutz muss alle Virentypen, Malware und Attacken im weiten Sinn abdecken.

Die Massnahmen sind auch auf die Mitarbeitenden im Homeoffice auszuweiten. Auf der Website des BACS sind dazu Empfehlungen zu finden[16].

Massnahmen:

- Die Arbeitsplätze sind so eingerichtet, dass die Bildschirme nicht von der Tür aus eingesehen werden können, damit Unberechtigte keinen Einblick in die Arbeit der Mitarbeitenden nehmen können.
- Gedruckte Dokumente liegen nicht unbeaufsichtigt beim Drucker herum. Dazu geben die Mitarbeitenden beispielsweise einen Code in den Drucker ein, der ihren Druckauftrag auslöst.
- Die Mitarbeitenden versorgen ihre gedruckten Dokumente und alle sensiblen Gegenstände (USB-Stick, CD-ROM usw.) in verschliessbaren Schränken oder Schubladen.
- Notebooks, allenfalls auch feste PC-Stationen, werden im Büro angekettet, damit sie nicht gestohlen werden können.
- Auf jedem PC ist ein Antivirus-Programm aktiviert und wird regelmässig aktualisiert.

[16] Home Office - Sicherer Zugang mit Fernzugriffen (admin.ch)

6.4 CLOUD-NUTZUNG

Eine Auslagerung von Daten findet heute üblicherweise in eine Cloud statt. Die Hauptgründe für die Nutzung von Cloud-Computing-Systemen sind die Reduktion der Kosten für IT-Infrastruktur und Software, das Outsourcing des Middleware- oder High-Level-Software-Managements, eine grössere Rechenkapazität, dynamischer Datenspeicherplatz (der in der Cloud gemietete Speicher passt sich automatisch der abgelegten Datenmenge an), die Mobilität, der einfache und rasche Datenzugang, die Erweiterbarkeit des Systems und in gewissen Fällen die Verbesserung der Sicherheit.

Die Delokalisierung von Daten ist immer mit Risiken behaftet. Problematisch ist Cloud-Computing in folgenden Hinsichten:

- Verlust der Kontrolle über die Daten;
- mangelnde Trennung und Isolierung der Daten verschiedener Kunden des Anbieters;
- Nichteinhaltung rechtlicher Bestimmungen durch den Anbieter;
- Datenzugang durch ausländische Behörden;
- Abhängigkeit.

Die folgenden Probleme bestehen, selbst wenn grundsätzlich in geringerem Ausmass, weiter, unabhängig davon, ob die Daten in der Cloud bearbeitet werden:

- Datenverlust;
- System- und Netzwerkausfälle und Nichtverfügbarkeit von Ressourcen und Diensten;
- missbräuchliche Datenverwendung.

Die Cloud-Nutzung ist kein Selbstzweck, sondern soll gewisse Bedürfnisse erfüllen. Diese müssen zuerst identifiziert werden. Dabei muss auch die Frage beantwortet werden, ob man wirklich eine Cloud benötigt, und falls ja, für welche Teile der Tätigkeit.

Im Übrigen ist bei der Wahl des infrage kommenden Cloud-Typs (private Cloud, unternehmenseigene öffentliche Cloud oder hybride Cloud) ausreichend frühzeitig eine vertiefte Analyse der Datenschutzanforderungen vorzunehmen, wobei der Bearbeitung von Personendaten (von deren Speicherung über eine spätere Bearbeitung bis zu deren Löschung) besondere Aufmerksamkeit zukommen muss, damit die Ausgestaltung der Cloud von Anfang an den Anforderungen entspricht. Falls nach der Risikoanalyse Zweifel bezüglich der Art der Bearbeitung von Personendaten in der Cloud bestehen, sollten diese nicht ohne weitere Risikominderungsmassnahmen delokalisiert werden.

Auch muss der Auftragsbearbeiter sorgfältig ausgewählt werden (anhand einer umfassenden Risikoanalyse aus organisatorischer, rechtlicher und technischer Sicht), mit präzisen Anweisungen instruiert und aufmerksam beaufsichtigt werden, wie Artikel 9 Absatz 2 DSG verlangt. Welche Anwendungen und Daten in eine Cloud ausgelagert werden können und welche auf eigenen Servern verbleiben müssen, ist sorgfältig abzuwägen. Schlussendlich bleibt der Cloud-Nutzer für die Einhaltung der Datenschutzvorschriften verantwortlich, wenn er einen Auftragsbearbeiter beauftragt hat, und er bleibt auch gegenüber den betroffenen Personen verantwortlich.

Weitere Erläuterungen zum Thema Cloud sind auf der Website des EDÖB zu finden[17].

[17] Cloud-Computing (admin.ch)

6.5 ZUR VERTIEFUNG

Weitere wichtige Aspekte, die bei der Infrastruktur zu beachten sind:

	CH-MS [1]	CNIL [8]	ISO 27002 [9]
Mobile-Device-Konfiguration	Ziff. 1.6.9	Ziff. 6	Ziff. 6.7
Elemente einer Defense-in-Depth-Strategie	Ziff. 1.6		
Hardware-Lifecycle-Management	Ziff. 1.6.8	Ziff. 13	Ziff. 7.14
Arbeitsplatzmanagement		Ziff. 5	Ziff. 7.6–7.8
Risikomanagement	Ziff. 1.6.3, 2.2.4–6		
Unterhalt (Maintenance)	Ziff. 2.3.5		Ziff. 7.13
Host Security	Ziff. 1.6.13		
Netzwerksicherheit		Ziff. 7, 8	Ziff. 8.20–8.22
Physische Sicherheit / Datensicherheit	Ziff. 1.6.7, 2.3.3	Ziff. 16	Ziff. 7.3–7.5

7 ZUGRIFF UND BEARBEITUNGEN

Die Datensicherheit, im Sinne von Artikel 8 DSG, Artikel 3 DSV sowie Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO, umfasst unter anderem auch die Sicherung des Datenzugriffs.

Die Vernichtung oder Anonymisierung der Daten, wenn für den Bearbeitungszweck nicht mehr benötigt, ist in Artikel 6 Absatz 4 DSG und Artikel 17 Absatz 1 Buchstabe a DSGVO geregelt.

Parallel zur Sicherung der Infrastruktur müssen auch Massnahmen auf Ebene der Datenverwendung und der -verwaltung ergriffen werden. Dieser Abschnitt befasst sich mit:

1. der Zugriffsverwaltung;
2. dem Lebenszyklus der Daten und der Protokollierung.

7.1 ZUGRIFFSVERWALTUNG

Bei der Zugriffsverwaltung geht es darum zu wissen, wer Zugriff auf die Daten hat und wer sie inwieweit bearbeiten darf. Das bringt unterschiedliche Sicherheitsanforderungen mit sich: Die Computer der Mitarbeitenden dürfen nur für die Personen mit Zugangsberechtigung zugänglich sein. Zudem müssen sie gegen jeglichen Zugriff von aussen geschützt werden. Solche Zugriffsversuche können vor Ort stattfinden – eine nicht berechtigte Person kommt in den Raum – oder von ausserhalb der Organisation – ein Unberechtigter greift über das Netz auf das System zu. Schliesslich muss entschieden werden, welche Spuren des physischen und des elektronischen Zugangs protokolliert werden:

1. Wie stellt man sicher, dass die Benutzerinnen und Benutzer identifiziert und authentifiziert werden?
2. Wie soll der Zugang zu den Benutzerdaten geschützt werden?
3. Wie lässt sich der Online-Zugang kontrollieren?

7.2 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

Durch die Identifizierung wird die Identität einer Person festgestellt. Man kann sie so von anderen unterscheiden. Mittels Authentifizierung wird überprüft, ob eine Person tatsächlich die ist, die sie zu sein vorgibt. Dafür gibt es drei Möglichkeiten: Eine Person kann sich anhand eines Gegenstandes, den sie auf sich trägt, authentifizieren lassen (z. B. eine Smartcard), oder anhand einer Information, die sie kennt (z. B. ein Passwort), oder anhand einer Eigenschaft, die sie auszeichnet (eine Verhaltenseigenschaft wie die Unterschrift oder eine physiologische Eigenschaft wie der Fingerabdruck). Man spricht von starker Authentifizierung oder Multi-Faktor-Authentifizierung (MFA), wenn mindestens zwei dieser Möglichkeiten zusammen benutzt werden müssen (z. B. Smartcard und Passwort, Passwort und Authenticator-App).

Passwortrichtlinien sind ein wichtiges Hilfsmittel der Authentifizierungsverwaltung. Sie verhindern, dass Mitarbeitende zu einfache Passwörter wählen, und reduzieren die damit verbundenen Risiken. Kriterien sind beispielsweise die Mindestlänge, die Ablaufzeit, die Verwendung von Sonderzeichen und Grossbuchstaben, die Anzahl Falscheingaben vor der Sperrung usw.

Programme zur Passwortgenerierung und -verwaltung können den Mitarbeitenden die Einhaltung der Vorgaben erleichtern.

Die CNIL stellt ein Merkblatt zur Authentifizierung[18] zur Verfügung, einschliesslich eines Instruments zur Berechnung der Komplexität der eigenen Passwortrichtlinien[19]. Auf der Website des BACS sind ausserdem spezifische Technologiebetrachtungen[20] zu finden (zurzeit nur auf Deutsch).

Massnahmen:

- Benutzerkonten, die die Authentifizierung erlauben, sind individuell. Auf ein Benutzerkonto kommt nur eine Person. Ein solches Konto umfasst eine identifizierende Zeichenfolge (Benutzername) und ein Passwort oder eine Smartcard usw.
- Idealerweise hat jede Person verschiedene Benutzerkonten, sodass sie sich zunächst beim Anschalten des Computers und dann wieder bei der Benutzung der verschiedenen Applikationen, mit denen sie arbeitet, authentifizieren muss. So kann eine Person in schlechter Absicht zwar auf den Computer zugreifen, durch den Schutz der Applikationen, aber nicht auf die Daten.
- Wenn mit einer einmaligen Authentifizierung gearbeitet wird (SSO), bedeutet der Zugang zur Maschine auch den Zugang zu den Applikationen. Deshalb müssen bei diesem System die Sicherheitsvorkehrungen angepasst werden.
- Detaillierte Passwortrichtlinien sind vorhanden und werden im Einklang mit der Entwicklung der Sicherheitsempfehlungen aktualisiert.
- Wie oft das Passwort geändert werden muss, hängt davon ab, wie hoch die Anforderungen an dessen Komplexität sind. Je komplexer das Passwort, desto weniger häufig muss es geändert werden und umgekehrt.
- Wer zur Authentifizierung biometrische Daten verwendet, muss sich an die Vorkehrungen halten, die im «Leitfaden zu biometrischen Erkennungssystemen» dargestellt sind.[21]

7.3 ZUGANG ZU DEN DATEN

Die Daten werden auf zentralen Servern gelagert. Die meisten Mitarbeitenden brauchen nicht Zugang zu allen Daten. Grenzt man ihren Zugang auf die Daten ein, die sie wirklich brauchen, verringert sich die Gefahr einer – bewussten oder unbewussten – Fehlbearbeitung. Einem Missbrauch der Daten kann ebenso vorgebeugt werden. Darum müssen Zugangsregeln und ein Autorisierungsmechanismus für alle Mitarbeitenden entsprechend ihrer Funktionen festgelegt werden.

Massnahmen:

- Das Informationssystem gewährt den Benutzerinnen und Benutzern differenzierte Zugangsrechte.
- Die interne Organisation legt für jede Mitarbeiterin und jeden Mitarbeiter die Zugangsrechte fest. Dazu erarbeitet sie eine Zugangsrechtematrix. Die Matrix wird regelmässig aktualisiert und bei Personalwechseln überprüft.
- Die Mitarbeitenden authentifizieren sich beim Anschalten des Systems. Je sensibler die Daten, die sie bearbeiten, desto höher sind die Anforderungen an die Authentifizierung.
- Der Zugang zu den Daten des Systems wird nach den Regeln des Abschnitts «Protokollierung» protokolliert.

[18] Sécurité : Authentifier les utilisateurs | CNIL
[19] Vérifier sa politique de mots de passe | CNIL
[20] Technologiebetrachtungen (admin.ch)
[21] Leitfaden zu biometrischen Erkennungssystemen (EDÖB)

7.4 ZUGANG VON AUSSERHALB DER ORGANISATION

Es gibt verschiedene Arten von Zugang zu den Daten von ausserhalb der Organisation. Entsprechend müssen jeweils spezifische Schutzvorkehrungen getroffen werden. So können Mitarbeitende um einen solchen Zugang ersuchen, weil sie ausserhalb arbeiten und von dort auf ihren Bürocomputer zugreifen möchte. Diese Art von Zugang muss gemäss der Politik der Organisation und der Sensibilität der Daten entsprechend mit einem System geregelt werden, das eine sichere Authentifizierung erlaubt. Weiter kann ein berechtigter Dritter wie ein Auftragsbearbeiter Zugang zu den Daten verlangen. Dieser Fall muss klar mit einer starken Authentifizierung geregelt werden. Missbräuchliche Zugriffe sind unbedingt zu verhindern.

Der Abschnitt «Netzsicherheit» enthält eingehendere Ausführungen zur Sicherheit der Kommunikation zwischen aussenstehenden Dritten und der Organisation.

Massnahmen:

- Den Personen, die von ausserhalb der Organisation auf die Daten zugreifen wollen oder müssen, wird ein geschützter Zugang eingerichtet.
- Die Authentifizierung beruht auf mindestens zwei Elementen. Sie ist also stark.
- Die persönlichen Computer sind mit einer Firewall geschützt.
- Die Zugriffe können unter den Voraussetzungen gemäss Abschnitt «Protokollierung» protokolliert werden.

7.5 ZUR VERTIEFUNG

Weitere wichtige Aspekte, die bei der internen Bearbeitung zu beachten sind:

	CH-MS [1]	CNIL [8]	ISO 27002 [2]
Analyse	Ziff. 2.5.3		Ziff. 5.24, 5.25
Risikoanalyse	Ziff. 2.2.4		
Benutzerauthentifizierung		Ziff. 2	Ziff. 8.5
Schadensminderung (Mitigation)	Ziff. 2.5.4		
Kommunikation	Ziff. 2.5.2, 2.6.3		
Physische Zugriffskontrolle	Ziff. 2.3.1		Ziff. 7.1, 7.2
Prüfung der Umsetzung und der Wirksamkeit der Massnahmen	Ziff. 3		Ziff. 5.35
Logische Zugriffskontrolle	Ziff. 2.3.1	Ziff. 3	
Definition der Umgebungen	Ziff. 2.2.2		Ziff. 8.31
Umgang mit Vorfällen und Datenverletzungen	Ziff. 2.4.1, 2.4.3	Ziff. 4	Ziff. 5.26
Risikomanagement	Ziff. 1.5.4		
Lieferketten-Risikomanagement	Ziff. 2.2.6		Ziff. 5.19
Vorgaben (Governance)	Ziff. 2.2.3		
Inventarmanagement	Ziff. 2.2.1		
Unterhalt (Maintenance)	Ziff. 2.3.5		
Organisation, Verantwortlichkeiten	Ziff. 1.5.2, 1.5.3		Ziff. 5.4
Reaktionsplanung	Ziff. 2.5.1		
Wiederherstellungsplanung	Ziff. 2.6.1		
Datensicherheit	Ziff. 2.3.3		
Sensibilisierung der Mitarbeitenden	Ziff. 1.6.17, 2.3.2	Ziff. 1	
Risikomanagementstrategie	Ziff. 2.2.5		Ziff. 5.24
Überwachung	Ziff. 2.4.2		Ziff. 8.15, 8.16
Sicherheit von Websites		Ziff. 9	
Sicherung und Archivierung		Ziff. 10, 11	Ziff. 8.15
Sicherer Austausch		Ziff. 15	

8 LEBENSZYKLUS DER DATEN

Werden die oben aufgeführten Massnahmen umgesetzt, so kann man davon ausgehen, dass der Zugang zu den Daten sowohl physisch (Zugang zu den Servern) als auch in Sachen Bearbeitung (Zugang zu den einzelnen Arbeitsplätzen und Anwendungen) sicherer ist. Nun geht es darum, diese Sicherheit während des ganzen Lebenszyklus der Daten zu gewährleisten. Die Daten müssen vom Moment ihrer Erstellung im System über alle Bearbeitungsschritte bis hin zu ihrer Vernichtung, Anonymisierung oder Archivierung unversehrt und vertrauenswürdig bleiben.

Sie können dabei innerhalb der Organisation von dazu Berechtigten oder aber auch von Drittorganisationen im Auftragsverhältnis bearbeitet werden.

Oft werden die Daten im Rahmen ihrer Bearbeitung zudem auf mobile Datenträger wie USB-Sticks, externe Festplatten usw. geladen. Es ist deshalb ratsam, die Bearbeitungen zu dokumentieren, die vorgenommen werden. Falls Unregelmässigkeiten auftauchen, ist so besser nachvollziehbar, wie sie entstanden sind.

Für die Verhinderung von Missbräuchen müssen alle diese Aspekte und Situationen unter die Lupe genommen werden.

Zu diesem Thema wird folgenden Fragen nachgegangen:

- Wie organisiert man die Erfassung der Daten im System?
- Wie werden die Daten verschlüsselt?
- Wie lässt sich die Sicherheit der verschiedenen Datenträger gewährleisten?
- Wie werden die Daten sicher aufbewahrt?
- Wie lassen sich Daten endgültig vernichten?
- Wie geht man mit der Informationssicherheit und dem Datenschutz um?
- Wie soll die Datenbearbeitung überwacht werden (Protokollierung)?
- Wie wird ein Bearbeitungsreglement erstellt?

8.1 DATENERFASSUNG

Ein erster heikler Punkt ist die Erfassung der Daten. Nebst verschiedenen Fragen der Sicherheit (siehe vor allem Infrastruktur und Zugriff und Bearbeitungen) gilt es, zu verhindern, dass unvollständige oder falsche Daten erfasst werden. Denn bei späteren Bearbeitungen kann sich daraus ein falsches Bild ergeben, was wiederum zu Fehlentscheiden führen kann.

Die Wahl der Eingabeplattform, die Datenzugriffsrichtlinien, die Validierung und die Verifizierung sind daher wichtige Elemente der Datenerfassung.

Zudem muss man klar unterscheiden, ob Daten in einem System erfasst werden, das gerade getestet wird, oder ob es bereits produktiv ist.

Massnahmen:

- Die Daten werden nur von dazu ausgebildeten und berechtigten Personen erfasst.
- Im System werden Hilfsmechanismen errichtet. Diese erkennen Informationslücken und führen allenfalls auf den erfassten Daten Wahrscheinlichkeitskontrollen durch.
- In einem Test werden nur Daten verwendet, die entweder fiktiv oder anonymisiert sind.
- Die Datenerfassung wird protokolliert (Protokollierung).

8.2 VERSCHLÜSSELUNG

Die Personendaten werden üblicherweise als Datei auf einer Festplatte oder in einer Datenbank gespeichert. Ihre Verschlüsselung verhindert, dass sie gelesen und missbräuchlich verändert werden: Mithilfe eines Schlüssels werden die Daten in einen unverständlichen Code umgewandelt. Wer den Schlüssel nicht kennt, kann die Daten somit nicht mehr entziffern.

Verschlüsselungsebenen

Die Verschlüsselung kann auf verschiedenen Ebenen erfolgen. Die gespeicherten Daten («at rest») sollten idealerweise jederzeit verschlüsselt sein. Die Verschlüsselung auf dieser Ebene schützt gegen Zugriff von aussen, beispielsweise bei Verlust der physischen Infrastruktur (Festplatte gestohlen oder vor der Entsorgung unzureichend gelöscht).

Da die Benutzerinnen und Benutzer wie auch die Anwendungen unverschlüsselte Daten benötigen, um sie bearbeiten zu können, ist empfohlen, intern eine zusätzliche Verschlüsselungsebene vorzusehen. Die Daten können auf verschiedene Zonen aufgeteilt werden, welche separat verschlüsselt werden und nur berechtigten Mitarbeitenden sowie Anwendungen den Zugriff auf die unverschlüsselten Daten gestatten. Diese Ebene schützt die Daten gegen unbefugte interne Zugriffe, beispielweise durch Mitglieder der Organisation, die unlautere Absichten haben oder gehackt wurden.

Die Verschlüsselung ist auch auf Dateiebene möglich, oder die schützenswerten Teile der Daten werden vom Rest getrennt verschlüsselt, was einen sehr granularen Schutz und damit die Nutzung der nicht schützenswerten Daten ermöglicht, ohne dass die anderen Daten gefährdet werden. Dies ist jedoch in der Umsetzung einiges komplexer.

Die geeignete Verschlüsselungsebene ist demnach abhängig von der vorgesehen Verwendung der Daten und ihrer Sensibilität zu bestimmen.

Wichtig ist auch, eine geeignete Verschlüsselungsmethode zu wählen und insbesondere keine mittlerweile obsoleten Methoden zu verwenden. Algorithmen, die zum Zeitpunkt der Erstellung dieses Leitfadens empfohlen werden, sind zum Beispiel:

- AES (mit einer Schlüssellänge von 128 oder 256 Bit) mit einem geeigneten Betriebsmodus (CCM, GCM oder EAX) oder ChaCha20 (im Poly-1305-Modus) für die symmetrische Verschlüsselung;
- RSA-OAEP, ECIES-KEM oder DLIES-KEM für die asymmetrische Verschlüsselung;
- SHA-256, SHA-512 oder SHA-3 als Hashfunktionen.

Ausführlichere Informationen sind auf der Website der ANSSI[22] zu finden.

[22] Mécanismes cryptographiques | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Massnahmen:

- Der Verschlüsselungsalgorithmus und insbesondere die Länge des Schlüssels sind proportional zur Sensibilität der Daten.
- Auf ein und demselben Datenträger können verschiedene Datengruppen mit je unterschiedlichen Schlüsseln verschlüsselt werden.
- Die Verschlüsselungsschlüssel werden gesichert.
- Nur eine begrenzte Anzahl Mitarbeitende hat Zugang zu den Schlüsseln.

8.3 SICHERHEIT DER DATENTRÄGER

Die Daten werden nicht nur auf zentralen Servern und PC gespeichert; zahlreiche externe Speichermedien ermöglichen den Transfer von Informationen unter Mitarbeitenden oder nach aussen, ohne dass dazu das Netz benützt werden muss. Diese Datenträger erlauben es auch, Daten vorübergehend und befristet aufzubewahren.

Solche externen Datenträger sind etwa USB-Sticks, externe Festplatten oder CD-ROM. Sie erfüllen aufgrund ihrer unterschiedlichen Eigenschaften auch unterschiedliche Funktionen. So sind z. B. USB-Sticks überschreibbar, CD-ROM nicht. Zudem passen immer mehr Daten auf immer kleinere Datenträger. Dies gilt es im Auge zu behalten, um die mit diesen Datenträgern verbundenen Risiken nicht zu unterschätzen.

Massnahmen:

- Die Mitarbeitenden erhalten eine Schulung zu den Gefahren, die das Anschliessen eines unbekannten externen Datenträgers an ihren PC mit sich bringen kann.
- Externe Datenträger, die besonders schützenswerte («sensible») Personendaten oder Persönlichkeitsprofile enthalten, werden verschlüsselt.
- Die externen Datenträger müssen unter Verschluss aufbewahrt werden.
- Ein Verfahren zur Vernichtung der Datenträger wird eingerichtet. Die dazu notwendigen Instrumente stehen zur Verfügung.
- Ein Verfahren zur korrekten und endgültigen Löschung der Daten auf dem Datenträger, sobald die Daten nicht mehr benötigt werden, wird eingerichtet. Die dazu notwendigen Instrumente stehen zur Verfügung.
- Eine regelmässige Kontrolle der Konfiguration und der Updates ist vorgesehen.

8.4 DATENSICHERUNG

Die Integrität und Verfügbarkeit der Daten eines Systems müssen sichergestellt werden. Daher ist ein Datensicherungsverfahren festzulegen. Wenn also beispielsweise eine Fehlmanipulation oder eine missbräuchliche Bearbeitung Daten vernichtet oder beschädigt, muss es möglich sein, die Daten so wiederherzustellen, wie sie vor dem Ereignis waren. Die Häufigkeit der Datensicherung muss auf die Anzahl Bearbeitungen, die pro Tag vorgenommen werden, abgestimmt sein.

Massnahmen:

- Es wird eine Sicherungsstrategie festgelegt, welche auf die Art der Daten, die Datenmenge und die Änderungshäufigkeit abstellt.
- Die Mitarbeitenden werden über die Sicherungsstrategie informiert.
- Die Sicherungsserver unterliegen den gleichen Sicherheitsmassnahmen wie die zentralen Server.
- Die Wiederherstellung von Daten wird Personen übertragen, die eigens dafür ausgebildet sind.

8.5 DATENVERNICHTUNG

Wie aus Artikel 6 Absatz 4 DSG hervorgeht, sollen Personendaten nicht auf unbeschränkte Zeit aufbewahrt zu werden. Die Aufbewahrungsdauer muss daher festgelegt und Mechanismen zur endgültigen Vernichtung müssen vorgesehen werden. Die Daten auf der Festplatte einfach zu löschen reicht nicht aus; sie dürfen nie mehr zugänglich sein, erst dann gelten sie als vernichtet. Das Gleiche gilt für Daten auf Papier oder auf mobilen Datenträgern. Auch die Sicherungskopien sind zu vernichten.

Massnahmen:

- Es wird eine geeignete Löschstrategie festgelegt, um eine schrittweise und vollständige Vernichtung der Personendaten sicherzustellen; diese umfasst auch Datensicherungen, die nicht mehr gebraucht werden.
- Die Daten werden mithilfe von Spezialsoftware gelöscht, die eine vollständige und endgültige Löschung der Daten garantiert (z. B. durch Bereinigen von leerem Speicherplatz).
- Daten auf Papier werden mit dem Aktenvernichter vernichtet.
- CD-ROM und andere mobile Datenträger werden ebenfalls physisch vernichtet, wenn sie nicht auf andere Weise vollständig bereinigt werden können.

8.6 SICHERHEITS- UND SCHUTZSTUFE

Um die Daten optimal zu schützen, kann es hilfreich sein, die Art der Personendaten mit einer Risikostufe und einer Klassifizierungsstufe in Beziehung zu setzen (z. B. «nicht klassifiziert, intern, vertraulich»). Ein Vorschlag für eine Klassifizierungsmatrix ist unten abgebildet. Es handelt sich um ein generisches Hilfsmittel. Die Matrix wird also nicht in jedem Fall adäquat sein und muss auf die organisationsspezifischen Bedürfnisse angepasst werden.

Tabelle 1: Massnahmenmatrix nach Vertraulichkeit und dem mit Personendaten verbundenen Risiko

Daten-schutz / Informations-schutz	Nicht personenbez. Daten	«Nicht-sensible» Personendaten	«Sensible» Personendaten	«Hochsensible» Personendaten
		Risiko: gering/mittel	Risiko: hoch	Risiko: sehr hoch
Nichtklassifizierte Information		**Zugang/Zugriff schützen**	Schützen **+ Verschlüsseln** **+ Bearbeitung protokollieren**	Schützen Verschlüsseln Protokollieren **+ Nummerieren***
INTERNE Information	**Zugang/Zugriff schützen**	Schützen	Schützen Verschlüsseln Protokollieren	Schützen Verschlüsseln Protokollieren Nummerieren
VERTRAULICHE Information	Schützen **+ Verschlüsseln**	Schützen Verschlüsseln	Schützen Verschlüsseln Protokollieren	Schützen Verschlüsseln Protokollieren Nummerieren
GEHEIME Information	Schützen Verschlüsseln **+ Nummerieren***	Schützen Verschlüsseln Nummerieren	Schützen Verschlüsseln Protokollieren Nummerieren	Schützen Verschlüsseln Protokollieren Nummerieren

* Die Nummerierung der Dokumente ist eine Massnahme zum Schutz der Information.

Im Beispiel der obigen Matrix werden die folgenden Risikodefinitionen verwendet:

1. ***Geringes Risiko:*** Personendaten, deren Missbrauch in der Regel für die betroffene Person keine besonderen Folgen hat, beispielsweise Name und Vorname oder öffentliche Informationen.
2. ***Mittleres Risiko:*** Personendaten, deren Missbrauch die wirtschaftliche Situation oder die gesellschaftliche Stellung der betroffenen Person beeinträchtigen kann. Dazu gehören beispielsweise Angaben über eine Mieterin oder einen Mieter oder über die beruflichen Verhältnisse einer Person oder auch ein Profiling.
3. ***Hohes Risiko:*** Personendaten, deren Missbrauch zu einer schweren Beeinträchtigung der wirtschaftlichen Situation oder der gesellschaftlichen Stellung führen kann. Dazu gehören besonders schützenswerte Personendaten und Profiling mit hohem Risiko.
4. ***Sehr hohes Risiko:*** «hochsensible» Personendaten, deren Missbrauch das Leben der betroffenen Person gefährden kann. Dazu gehören Adressen von V-Leuten der Polizei, von Zeuginnen und Zeugen in bestimmten Strafverfahren oder von Personen, die aufgrund ihrer Gesinnung oder ihrer religiösen oder politischen Zugehörigkeit bedroht sind.

Massnahmen:

- Das System wird anhand einer angepassten Matrix erarbeitet.
- Die ergriffenen Massnahmen entsprechen der Matrix.

8.7 PROTOKOLLIERUNG

Es ist in der Regel von grossem Nutzen zu wissen, welche Bearbeitungen mit welchen Daten vorgenommen worden sind, egal, ob es sich dabei um die Abfrage von Daten, die Erfassung neuer oder die Änderung oder Vernichtung bestehender Daten handelt. Wenn ein Problem auftaucht, erlauben solche Aufzeichnungen herauszufinden, wo ein Zwischenfall (unbefugter Zugriff, unbefugte Bearbeitung von Daten usw.) stattgefunden hat.

Diese einzelnen Handlungen können protokolliert werden; alle Ereignisse im Zusammenhang mit dem Informationssystem werden sequenziell aufgezeichnet. Die Aufbewahrungszeit dieser Protokolldateien («Logfiles») bestimmt sich nach der Sensibilität der Daten und der Bearbeitungen sowie nach den Bearbeitungszwecken.

Die Protokollierung ist in Artikel 4 DSV geregelt: Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der private Verantwortliche und sein privater Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren.

Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

Die Protokolldateien müssen spezifische Anforderungen erfüllen:

- Sie müssen getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden.
- Sie müssen während mindestens einem Jahr aufbewahrt werden.
- Sie dürfen ausschliesslich einem eingeschränkten Personenkreis zugänglich sein, namentlich jenen Personen, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

Bei Personendaten, welche allgemein öffentlich zugänglich sind, sind zumindest das Speichern, Verändern, Löschen und Vernichten der Daten zu protokollieren.

Sämtliche Bearbeitungen von Personendaten zu protokollieren, ist sehr aufwändig. Um die Einrichtung eines Protokollierungsprotokolls zu erleichtern und besser zu erkennen, ob die Pflicht dazu besteht, werden im Folgenden einige häufig gestellte Fragen beantwortet:

- Es wird keine getrennte Protokollierung der Personendaten und der Informationssicherheit erwartet. Eine Redundanz ist folglich nicht nötig.
- Die Protokollierungspflicht gilt ausschliesslich für Personendaten in Systemen zur automatisierten Datenbearbeitung. Beispielsweise muss ein manueller Zugriff auf ein Textdokument mit persönlichen Informationen gemäss Artikel 4 DSV nicht zwingend protokolliert werden. Wird hingegen im gleichen Dokument ein Skript ausgeführt, das Personendaten löscht, so muss dies protokolliert werden.

    - Nichtsdestotrotz muss aber beachtet werden, dass es im Interesse des Verantwortlichen sein kann, diese Aktivitäten gleichwohl zu protokollieren oder die Bearbeitung gewisser Personendaten in nicht protokollierten Dokumenten nicht zuzulassen.
- Unter «allgemein öffentlich zugänglich» sind Daten zu verstehen, die ohne Identifizierung oder die einer grossen Zahl von Personen zugänglich sind.

Weitere Informationen zur Protokollierung sind auf der Website des BACS erhältlich[23].

Ein solches Protokoll kann auch freiwillig ins System integriert werden. Die Protokollierung muss dabei aber klar notwendig sein und präzise umschriebenen Zwecken dienen; es gilt zu vermeiden, einfach unbegründet zusätzliche Daten – und damit zusätzliche Risiken – zu generieren. Die Menge protokollierter Informationen und die Aufbewahrungsdauer für die Logfiles müssen verhältnismässig sein.

Massnahmen:

- Inhalt und Aufbewahrungsdauer der Logfiles stehen in einem Verhältnis zu den Daten und den vorgenommenen Bearbeitungen.
- Die Mitarbeitenden werden darüber informiert, dass die Spuren jedes Vorgangs, der Daten betrifft, aufbewahrt werden.
- Die Datensammlungen, die durch die Protokollierung entstehen (Protokolle), werden gesichert.
- Die Zugriffsrechte auf die Protokolle werden klar umschrieben und auf bestimmte Funktionen innerhalb der Organisation beschränkt.
- Das Protokoll wird gegen allfällige Attacken und unbefugte Zugriffe geschützt.

8.8 BEARBEITUNGSREGLEMENT

Das Instrument des Bearbeitungsreglements wird in den Artikeln 5 und 6 DSV geregelt. Ein Bearbeitungsreglement (in Form einer Anleitung oder einer Dokumentation) enthält Angaben zur internen Organisation, beispielsweise die Beschreibung der Systemarchitektur; zum Datenbearbeitungsverfahren, insbesondere zur Bekanntgabe der Daten und zur Ausübung des Auskunftsrechts; zum Kontrollverfahren (Berechtigungen) sowie zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit.

Das Bearbeitungsreglement muss vom Verantwortlichen und seinem Auftragsbearbeiter erstellt werden. Sofern es obligatorisch ist, muss es auch regelmässig aktualisiert und der Datenschutzberaterin oder dem Datenschutzberater zur Verfügung gestellt werden.

Pflicht zur Führung eines Reglements und Inhalt

Der private Verantwortliche ist verpflichtet, ein Reglement für automatisierte Bearbeitungen zu erstellen, wenn er besonders schützenswerte Personendaten in grossem Umfang bearbeitet oder ein Profiling mit hohem Risiko durchführt. Das Reglement muss insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten (Art. 5 DSV).

Wenn der Verantwortliche ein Bundesorgan ist (Art. 6 DSV), so erstellt er ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn er:

a. besonders schützenswerte Personendaten bearbeitet;
b. ein Profiling durchführt;

[23] Technische Empfehlungen für die Protokollierung gemäss Art. 4 DSV des EDÖB

c. nach Artikel 34 Absatz 2 Buchstabe c DSG Personendaten bearbeitet;
d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen Personendaten zugänglich macht;
e. Datenbestände miteinander verknüpft;
f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaftet.

Weitere Informationen zum Bearbeitungsreglement sind auf der Website des EDÖB verfügbar[24].

[24] Bearbeitungsreglement (Private) (DOCX)

9 DATENAUSTAUSCH UND -ÜBERMITTLUNG

Der Grundsatz der Verhältnismässigkeit (Art. 6 Abs. 2 DSG und Art. 5 Abs. 1 Bst. c DSGVO) beinhaltet die Einschränkung des Zugangs zu Personendaten.

Die Artikel 9 DSG und 7 DSV enthalten allgemeine Vorschriften zum Schutz von Personendaten im Rahmen der Bearbeitung durch Auftragsbearbeiter.

Die heutige Kommunikationstechnologie ermöglicht es, via Internet zu arbeiten und rasch und einfach Informationen auszutauschen. Dadurch bleiben die Daten nicht mehr einfach in der Organisation, sondern werden nach aussen übermittelt. Regelmässig kommt es zu einem Austausch mit Dritten. Der Datenschutz muss auch bei der Übermittlung sichergestellt sein.

In diesem Abschnitt werden die folgenden Fragen behandelt:

- Wie lässt sich eine ausreichende Sicherheit garantieren?
- Wie ist eine Mitteilung zu verschlüsseln, die einer Drittperson übermittelt wird?
- Wie ist eine Mitteilung digital zu unterzeichnen, die einer Drittperson übermittelt wird?
- Wie können mobile Datenträger sicher weitergegeben werden?
- Wie sind die verschiedenen Informationstransfers zu protokollieren?
- Was sind die Besonderheiten der Datenübermittlung ins Ausland?

9.1 NETZSICHERHEIT

Die Datentransfers in den internen Netzwerken einer Organisation sind zahlreich. So kann es Mitarbeitende geben, die ausserhalb der Organisation arbeiten und Zugang zum Intranet haben, oder Dritte, die so auf die Daten zugreifen können. In der Regel erfolgt der Zugang über das Internet; dabei muss die Sicherheit des Netzes und der Kommunikation gewährleistet sein. Es müssen unbedingt gesicherte Übertragungsprotokolle verwendet werden. Das TLS-Protokoll (Transport Layer Security), Nachfolger des SSL-Protokolls (Secure Sockets Layer), ist ein Verschlüsselungsprotokoll, das den gesicherten Datenaustausch zwischen Client und Server erlaubt. Die Algorithmen und die kryptografischen Schlüssel werden zwischen Client und Serverbetreiber ausgehandelt. Das TLS-Protokoll erlaubt zudem, die beiden Parteien mithilfe von Zertifikaten zu authentifizieren. Dieses Protokoll befindet sich in einer Schicht unterhalb der üblichen Übertragungsprotokolle (HTTP, FTP usw.). Es ist für die Benutzerinnen und Benutzer transparent, die Anwendung kann im Bearbeitungsfenster der meisten Browser mit einem Schlosssymbol angezeigt werden.

Auch VPN-Verbindungen (virtuelles Privatnetzwerk) tragen zur Sicherung des Intranet-Zugangs bei. Über solche Verbindungen werden die verschlüsselten Daten, die übermittelt werden sollen, eingekapselt. Ein VPN fusst auf strengen kryptografischen Protokollen wie TLS, IPSec oder SSTP.

Massnahmen:

- Der Übermittlung von Daten aus dem Intranet via Internet nach aussen ist auf das strikte Minimum zu beschränken.
- Prüfen, ob die Erstellung eines sicheren Kommunikationsprotokolls (z. B. TLS) für die Bearbeitung der Daten vorgesehen ist.
- Müssen Mitarbeitende oder Dritte von ausserhalb der Organisation auf das Intranet der Organisation zugreifen, ein VPN einrichten.

- Täglich die Updates der verschiedenen verwendeten Programme kontrollieren und sicherstellen, dass sie durchgeführt werden, um das maximale Sicherheitsniveau zu erhalten.

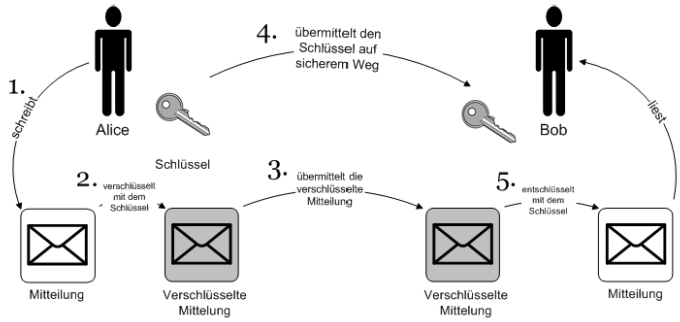
9.2 VERSCHLÜSSELUNG VON MITTEILUNGEN

Neben der Festplatte und den Dateien sind gleichzeitig auch die Mitteilungen zu verschlüsseln. Nur so lässt sich ein unerwünschter Zugriff auf die Daten verhindern und vermeiden, dass unberechtigte Dritte eine Mitteilung lesen, verändern oder löschen können.

Es gibt zwei Möglichkeiten, um Mitteilungen zu chiffrieren: die symmetrische und die asymmetrische Verschlüsselung.

Die symmetrische Verschlüsselung funktioniert nach untenstehendem Schema:

1. Alice schreibt Bob eine Mitteilung.
2. Alice chiffriert die Mitteilung mit einem Schlüssel.
3. Alice übermittelt Bob die verschlüsselte Mitteilung.
4. Alice übermittelt Bob den Schlüssel dazu auf sicherem Weg.
5. Bob verwendet diesen Schlüssel, um die Mitteilung zu dechiffrieren.

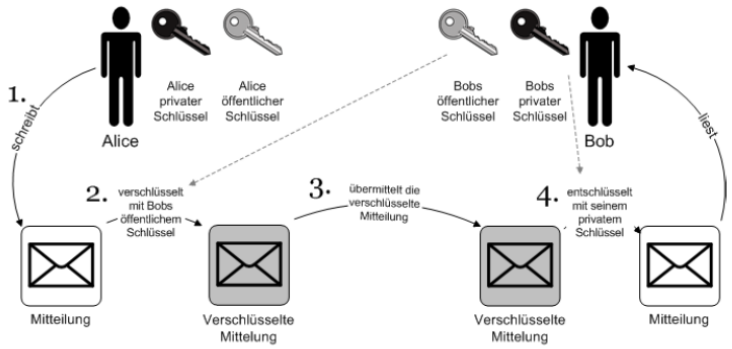


Die symmetrische Verschlüsselung ist ein schnelles Verfahren, welches auf grosse Datenmengen ausgelegt ist. Sie lässt sich einfach umsetzen, weil es nur einen Schlüssel dazu braucht. Allerdings ist darauf zu achten, dass dieser Schlüssel auf sichere Art und Weise übergeben wird.

Die asymmetrische Verschlüsselung ist komplexer und daher auch langsamer. Sie löst aber das Sicherheitsproblem, das mit der Übergabe des Schlüssels verbunden sein kann. Statt eines einzigen Schlüssels erzeugt jede Benutzerin und jeder Benutzer nämlich zwei Schlüssel. Der eine davon ist öffentlich und für alle zugänglich, der andere ist privat, und nur die betreffende Person kennt ihn. Der öffentliche Schlüssel wird zur Verschlüsselung der Mitteilung verwendet, der private Schlüssel für deren Entschlüsselung. Dank dieser Technik können Mitteilungen auch digital signiert werden (vgl. Abschnitt «Unterzeichnen von Mitteilungen»).

Und so läuft die asymmetrische Verschlüsselung ab:

1. Alice bereitet eine Mitteilung für Bob vor.
2. Alice benutzt Bobs öffentlichen Schlüssel zur Chiffrierung der ganzen Mitteilung. Damit stellt sie sicher, dass nur Bob die Mitteilung lesen kann.
3. Alice stellt Bob die Mitteilung zu.
4. Bob verwendet seinen privaten Schlüssel zur Entschlüsselung der Mitteilung.



Viele Anwendungen verwenden heutzutage keinen reinen asymmetrischen Verschlüsselungsalgorithmus, sondern sie verschlüsseln die Daten mit einem symmetrischen Algorithmus und verschlüsseln zusätzlich den symmetrischen Verschlüsselungsschlüssel mit einem asymmetrischen Verschlüsselungsalgorithmus. Diese hybride Verschlüsselungsmethode kombiniert die Vorteile: Die Schnelligkeit der symmetrischen und die Sicherheit der asymmetrischen Verschlüsselung.

Massnahmen:

- Entscheiden, welche Art von Verschlüsselung die geeignete ist. Zu berücksichtigen sind dabei die Datenmenge, die Sensibilität der Daten und die Drittpersonen, mit denen die Organisation zu tun hat.
- Wird die symmetrische Verschlüsselung benutzt, so ist ein sicheres Protokoll für die Übermittlung des Schlüssels vorzusehen (E-Mail beispielsweise ist nicht sicher).
- Wird die asymmetrische Verschlüsselung gewählt, so muss ein Verschlüsselungsmechanismus eingerichtet werden. Sinnvoll ist, diesen Mechanismus an die Unterschrift von Mitteilungen zu koppeln (vgl. Abschnitt «Digital Unterzeichnen von Mitteilungen»).

Nun muss Alice noch überprüfen, dass der öffentliche Schlüssel, über den sie verfügt, wirklich jener von Bob ist – und nicht einer Person dazwischen gehört («man in the middle»). Dazu kann der öffentliche Schlüssel von Bob von einer höheren Autorität signiert sein, deren öffentlicher Schlüssel wiederum signiert sein kann und so weiter, bis zu einer Alice bekannten und durch sie verifizierbaren Stufe. Das Signieren von Mitteilungen oder öffentlichen Schlüsseln wird im nächsten Abschnitt erläutert.

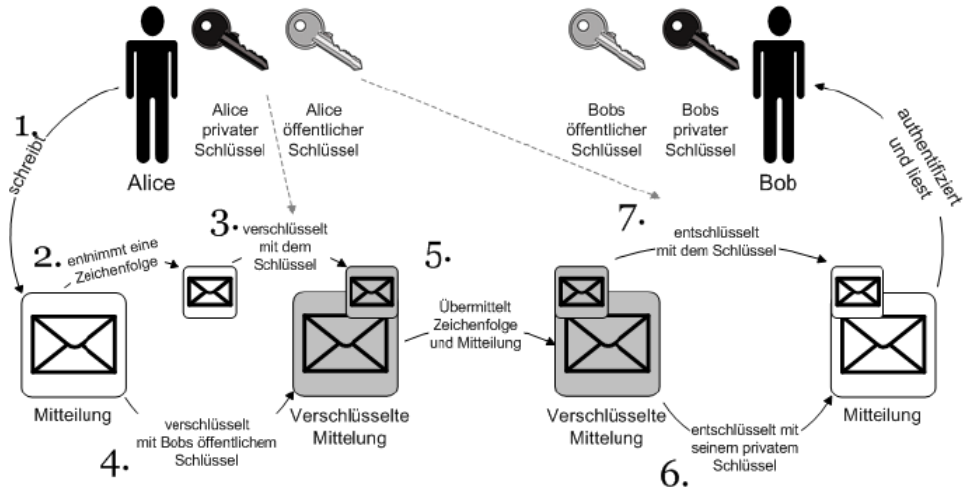
9.3 Digital Unterzeichnen von Mitteilungen (Signieren)

Die Verschlüsselung einer Mitteilung (vgl. Abschnitt «Verschlüsselung von Mitteilungen») stellt sicher, dass nur die Person die Mitteilung lesen kann, die den für die Dechiffrierung erforderlichen Schlüssel besitzt. Es kann aber auch notwendig sein, dass der Adressat der Mitteilung sich versichern muss, dass die Absenderin tatsächlich die Person ist, die sie zu sein vorgibt. Mit der digitalen Unterschrift auf der Mitteilung kann die Absenderin diese Information sicher übermitteln.

Die digitale Unterzeichnung wird üblicherweise vor der Verschlüsselung vorgenommen und zwar nach folgendem Ablauf:

1. Alice schreibt eine Mitteilung.
2. Alice entnimmt ihrer Mitteilung eine Zeichenfolge. Diese Zeichenfolge dient als Unterschrift für die Mitteilung.

3. Alice unterschreibt diese Zeichenfolge mit ihrem privaten Schlüssel.
4. Dann chiffriert sie die Mitteilung nach dem oben beschriebenen Verfahren.
5. Alice übermittelt Bob die Zeichenfolge und die Mitteilung.
6. Bob entschlüsselt die Mitteilung.
7. Schliesslich überprüft er die Zeichenfolge mit dem öffentlichen Schlüssel von Alice und versichert sich damit, dass sie es war, die ihm die Mitteilung zugestellt hat.



Massnahmen:

- Die Mitarbeitenden werden für die Situationen sensibilisiert, in denen sie ihre Informationen digital unterzeichnen und verschlüsseln müssen.
- Die Mitarbeitenden wissen, wie Mitteilungen verschlüsselt und signiert werden.

9.4 ÜBERGABE VON DATENTRÄGERN

Die Übergabe mobiler Datenträger ist heikel, denn damit verlässt ein Teil der Daten physisch die Organisation und wird an einen anderen Ort transportiert. Es ist von zentraler Bedeutung, dass diese Datenträger während ihres Transports so geschützt werden, dass die Daten bei einem Verlust des Datenträgers oder – schlimmer – bei einem Diebstahl nicht zugänglich sind. Je schützenswerter die Daten auf dem mobilen Datenträger sind, desto besser muss der Transport gesichert werden.

Massnahmen:

- Die Empfängerinnen und Empfänger von mobilen Datenträgern können sicher authentifiziert werden.
- Die mobilen Datenträger werden vor dem Transport sicher verpackt.
- Wenn nötig werden die mobilen Datenträger verschlüsselt.
- Das Vorgehen für den Transport ist klar festgelegt. Zum Beispiel dürfen mobile Datenträger nur in verschlossenen Koffern oder Taschen transportiert werden.
- Dank dem Vier-Augen-Prinzip kann besser sichergestellt werden, dass Übergabe und Empfang von Daten korrekt vonstattengehen.

9.5 PROTOKOLLIERUNG DES DATENAUSTAUSCHS

Das Übermitteln von Daten via Internet und die Übergabe von mobilen Datenträgern können protokolliert und in einem Journal festgehalten werden. Auf diese Weise lassen sich Absender und Adressaten ebenso nachvollziehen wie die Übergabe der mobilen Datenträger. Bei einem Missbrauch, einer falschen Verwendung oder einer Fehlmanipulation kann anhand dieser Informationen der Weg, den die Daten von der Übergabe bis zum Eintreten des Problems zurückgelegt haben, nachvollzogen werden.

Die Anforderungen gemäss Abschnitt «Protokollierung» gelten auch für die Protokollierung des Datenaustauschs.

Massnahmen:

- Sehr genau definieren, wie die Absender und Empfänger, der Weg, den die Daten zurücklegen, und alle wichtigen Punkte dieses Weges protokolliert werden.
- Vorzugsweise sollte der Transfer mobiler Datenträger immer den gleichen Mitarbeitenden anvertraut werden.
- Für die Protokollierung gilt das Verhältnismässigkeitsprinzip. Die Protokollierung der Datenaustauschs richtet sich nach Umfang, Dauer usw.

9.6 DATENBEKANNTGABE INS AUSLAND

Die Bekanntgabe von Personendaten ins Ausland birgt grosse Risiken: Sie wird daher in den Artikeln 16–18 DSG und den Artikeln 8–12 DSV relativ detailliert geregelt. Grundsätzlich sollten Personendaten nicht ins Ausland übermittelt werden. Grob gesagt gibt es aber drei Arten von Situationen, in denen eine solche Bekanntgabe dennoch zulässig ist:

Genehmigung des Bundesrats

Der erste Fall ist in Artikel 16 Absatz 1 DSG und Artikel 8 DSV festgehalten. Der Bundesrat erstellt eine Positivliste der Staaten, deren Datenschutzgesetzgebung als angemessen beurteilt wird. Ist ein Staat nicht auf der Liste aufgeführt, so wurde seine Gesetzgebung entweder als ungenügend eingestuft oder aber noch nicht beurteilt. Neben Staaten kann es sich auch um internationale Organe handeln. Die Liste ist in Anhang 1 DSV zu finden[25].

Spezifische Instrumente

Der zweite Fall ist in Artikel 16 Absatz 2 DSG und Artikel 9 ff. DSV geregelt. Ist der betreffende Staat nicht auf der erwähnten Liste aufgeführt, gibt es verschiedene Datenschutzinstrumente, deren Verwendung die Datenbekanntgabe in diesen Staat erlauben. Das Gesetz nennt die folgenden Instrumente:

- ein völkerrechtlicher Vertrag;
- Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden;
- spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat;
- Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat;

[25] Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutz

– verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.

Nach Artikel 12 DSV kommen zu dieser Liste noch Verhaltenskodizes und Zertifizierungen hinzu, die unter gewissen Voraussetzungen eine Bekanntgabe von Daten ins Ausland begründen können.

Ausnahmen
Der dritte Fall ist in Artikel 17 DSG festgelegt. Ausser in den oben dargestellten Situationen kann eine Datenbekanntgabe ins Ausland in gewissen Spezialfällen zulässig sein: Es handelt sich im Wesentlichen um Situationen, in denen die betroffene Person in gewisser Weise in die Übermittlung einbezogen ist oder die Übermittlung die Wahrung wichtiger Interessen bezweckt. Das DSG sieht die folgenden Fälle vor:

– Die betroffene Person hat in die Bekanntgabe eingewilligt.
– Die betroffene Person hat die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt.
– Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person.
– Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person.
– Die Bekanntgabe ist notwendig für die Wahrung eines überwiegenden öffentlichen Interesses.
– Die Bekanntgabe ist notwendig für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde.
– Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.
– Die Daten stammen aus einem gesetzlich vorgesehenen Register, das öffentlich oder Personen mit einem schutzwürdigen Interesse zugänglich ist, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind.

Ausserdem muss der Verantwortliche in gewissen Fällen den EDÖB auf Anfrage über die Bekanntgabe von Personendaten informieren (Art. 17 Abs. 2 DSG).

Massnahmen:

- Bereits ab der Konzeption und vor jeglicher Bekanntgabe den Anforderungen und den Risiken einer Datenbekanntgabe ins Ausland Rechnung tragen.
- Regelmässig die Länderliste in Anhang 1 DSV konsultieren.
- Bei Bedarf prüfen, ob der Einsatz eines der oben aufgeführten Instrumente möglich und angezeigt ist.

9.7 BEARBEITUNG DURCH AUFTRAGSBEARBEITER

Es kommt regelmässig vor, dass eine Organisation in Zusammenhang mit der Verwaltung der von ihr bearbeiteten Daten Auftragsbearbeiter beizieht. Als Beispiel zu nennen sind etwa die Datenspeicherung bei Dritten, die Nutzung von IT-Lösungen, die von einer Drittfirma erbracht

und von ihr gewartet werden (namentlich via Cloud), oder genereller die Übertragung einer bestimmten Aufgabe, wie der Rechnungsstellung, der Kundenwerbung o. ä. Die Organisation, die den Auftrag vergibt, muss sich dabei vergewissern, dass der Auftragsbearbeiter in der Lage ist, den Datenschutz angemessen zu gewährleisten (Art. 9 Abs. 2 DSG). Zudem bleibt sie für die Bearbeitung und damit gegenüber den betroffenen Personen und den Behörden verantwortlich.

Der Verantwortliche darf Personendaten nur übermitteln, wenn dies gesetzlich oder vertraglich vorgesehen ist. Zudem darf der Dritte die Daten nur so bearbeiten, wie der Verantwortliche selbst es tun dürfte. Schliesslich darf auch keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbieten (Art. 9 Abs. 1 DSG). Zu beachten ist ausserdem, dass der Auftragsbearbeiter die Bearbeitung seinerseits nur mit Genehmigung des Verantwortlichen einem Dritten übertragen darf (Art. 9 Abs. 3 DSG).

Massnahmen:

- Die Zuverlässigkeit des Angebots von Auftragsbearbeitern, ihre Reputation und ihre Expertise im Bereich Datensicherheit und Datenschutz überprüfen.
- Mit dem Auftragsbearbeiter einen Vertrag abschliessen, der die Datenbearbeitung durch diesen regelt und mit dem die Einhaltung der Pflichten des Verantwortlichen gegenüber den betroffenen Personen (Vertraulichkeit der Daten, Herausgabe- und Vernichtungsbedingungen, Incident-Management, Auskunftsbegehren usw.) sichergestellt werden kann.
- Mechanismen vorsehen, mit denen gewährleistet werden kann, dass der Auftragsbearbeiter seinen Verpflichtungen im Datenschutzbereich nachkommt (Sicherheitsaudits, Datenverschlüsselung nach Sensibilität usw.).

Empfehlungen und zusätzliche Hilfsmittel sind auf der Website des BACS[26] zu finden.

10 SCHLUSSBEMERKUNGEN

Die in diesem Leitfaden dargestellten technischen und organisatorischen Massnahmen ermöglichen den angemessenen Schutz der Daten. Allerdings müssen immer auch weitere Faktoren wie beispielsweise das globale Umfeld eines konkreten Projekts, dessen Sensibilität oder die Menge der notwendigen Daten mitberücksichtigt werden.

Der Datenschutz ist Sache des Verantwortlichen. Das Thema bei der Entwicklung eines Projekts möglichst frühzeitig anzugehen, ist der beste Weg, um nicht nur die verschiedenen Risiken bewältigen zu können, sondern vor allem auch, um seinen diversen Pflichten gegenüber den betroffenen Personen nachkommen zu können.

[26] Empfehlungen für die Zusammenarbeit mit IT-Providern

11 REFERENZEN

[1] Bundesamt für wirtschaftliche Landesversorgung (BWL), «IKT-Minimalstandard», 2023. [Online]. Available: https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html. [Zugriff am 25. August 2023].

[2] ISO, «Standards» [Online]. Available: https://www.iso.org/standards.html. [Zugriff am 29. August 2023].

[3] ISACA, «COBIT | Control Objectives for Information Technologies | ISACA» [Online]. Available: https://www.isaca.org/resources/cobit. [Zugriff am 29. August 2023].

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), «Technische Richtlinien» [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html. [Zugriff am 29. August 2023].

[5] NIST, «National Institute of Standard and Technology» [Online]. Available: https://www.nist.gov/. [Zugriff am 29. August 2023].

[6] CNIL, «Privacy Impact Assessment - Knowledge Bases», Februar 2018. [Online]. Available: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf. [Zugriff am 25. August 2023].

[7] Artikel-29-Datenschutzgruppe, «Stellungnahme 05/2014 zu Anonymisierungstechniken», 10. April 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf. [Zugriff am 25. August 2023].

[8] CNIL, «Guide pratique RGPD - Sécurité des données personnelles», April 2023. [Online]. Available: https://www.cnil.fr/sites/cnil/files/2023-04/cnil_guide_securite_des_donnees_personnelles-2023.pdf. [Zugriff am 25. August 2023].

[9] International Organization for Standardization, «Information security, cybersecurity and privacy protection – Information security controls», 2022. [Online]. Available: https://www.iso.org/standard/75652.html. [Zugriff im September 2023].