



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes

August 2015

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch



Inhaltsverzeichnis

Einleitung	3
Begriffe	3
Daten-/Informationssicherheit	3
Datenschutz	3
Informationsschutz	3
Personendaten	4
Datensammlung	4
Zuständigkeiten	5
Gesetzliche Grundlagen	5
Technische und organisatorische Massnahmen	5
Inhalt des Leitfadens	6
Schwerpunkt A. Zugang zu den Daten	7
A.1 Sicherheit der Räumlichkeiten	8
A.2 Sicherheit der Serverräume	9
A.3 Sicherheit des Arbeitsplatzes	9
A.4 Identifizierung und Authentifizierung	10
A.5 Zugang zu den Daten	11
A.6 Zugang von ausserhalb der Organisation	12
Schwerpunkt B. Lebenszyklus von Daten	13
B.1 Datenerfassung	14
B.2 Protokollierung	14
B.3 Pseudonymisierung und Anonymisierung	15
B.4 Verschlüsselung	17
B.5 Sicherheit der Datenträger	17
B.6 Datensicherung	18
B.7 Datenvernichtung	18
B.8 Auslagerung von Arbeiten (Bearbeitung durch Dritte)	19
B.9 Sicherheit und Schutz	19
Schwerpunkt C. Datenaustausch	21
C.1 Netzsicherheit	22
C.2 Verschlüsselung von Mitteilungen	22
C.3 Unterzeichnen von Mitteilungen	24
C.4 Übergabe von Datenträgern	26
C.5 Protokollierung des Datenaustauschs	26
Schwerpunkt D. Auskunftsrecht	27
D.1 Recht der betroffenen Personen	27
D.2 Reproduzierbarkeit der Verfahren	28
Hilfsmittel	29
Evaluationsraster	29
Das Bearbeitungsreglement	29
Inhalt des Reglements	29
Schlussbemerkung	30



EINLEITUNG

Dieser Leitfaden führt in die Gefahren ein, welche die modernen Informationssysteme aus der Sicht des Datenschutzes mit sich bringen. Er soll dabei helfen, Massnahmen zu realisieren, die einen optimalen und angemessenen Schutz der Personendaten sicherstellen. Die wichtigsten Themen des Datenschutzes werden ebenso dargestellt wie die damit verbundenen technischen und organisatorischen Massnahmen Verschlüsselung, Anonymisierung und Authentifizierung.

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 oder Techniker sind oder nicht. Jedoch dürften auch andere Interessierte darin Antworten auf ihre Fragen finden.

Der Leitfaden gliedert sich um die vier Schwerpunktthemen Zugang zu Daten, Lebensdauer von Daten, Datenübermittlung und Auskunftsrecht. Zu jedem Thema werden die Aspekte dargestellt, die beim Entwurf und bei 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.

Begriffe

Zur besseren Verständlichkeit des Leitfadens folgen zunächst einige Begriffserklärungen:

Daten-/Informationssicherheit

- Die **Daten-/Informationssicherheit** umfasst alle Massnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten/Informationen.

Datenschutz

- Der **Datenschutz** umfasst alle Massnahmen zur Verhinderung einer unerwünschten Bearbeitung von Personendaten und deren Folgen.

Informationsschutz

- Der **Informationsschutz** legt, im Hinblick auf die Wahrung der Interessen eines Landes oder einer Organisation, die Vertraulichkeitsstufen für Informationen (INTERN, VERTRAULICH, GEHEIM) fest.



Personendaten

- Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, sind **Personendaten**. Sie werden als **nicht-sensible Personendaten** bezeichnet, wenn sie keine besondere Schutzwürdigkeit (siehe untenstehende Definition) aufweisen.
- **Besonders schützenswerte („sensible“) Personendaten** sind Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe und über administrative oder strafrechtliche Verfolgungen und Sanktionen. Wenn das Bekanntwerden solcher Daten zur Bedrohung, insbesondere an Leib und Leben der betroffenen Person führen kann, dann spricht man von **hochsensiblen** (lebenswichtigen) **Personendaten**.
- Ein **Persönlichkeitsprofil** ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
- Die **betroffene Person** ist die natürliche oder juristische Person, über die Daten bearbeitet werden.
- Für Personendaten gibt es vier **Risikostufen**:
 1. **Geringes Risiko**: Personendaten, deren Missbrauch in der Regel für die betroffene Person keine besonderen Folgen hat, beispielsweise Name, Vorname, Adresse und Geburtsdatum oder Informationen, die in den Medien erschienen sind, soweit sie nicht in einem sensiblen Zusammenhang stehen
 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.
 3. **Hohes Risiko**: Personendaten, deren Missbrauch zu einer schweren Beeinträchtigung der wirtschaftlichen Situation oder der gesellschaftlichen Stellung führen kann. Dazu gehören Daten zur Gesundheit, besonders schützenswerte („sensible“) Personendaten und Persönlichkeitsprofile.
 4. **Sehr hohes Risiko**: 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.

Datensammlung

- Nach schweizerischem Recht ist eine **Datensammlung** jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.



Zuständigkeiten

Für eine Organisation, die Personendaten bearbeitet, sind folgende Funktionen wichtig:

- **Inhaberin oder der Inhaber der Datensammlung** sind private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden.
- Der oder die **Datenschutzverantwortliche** überwacht innerhalb einer Organisation die Einhaltung der Datenschutzvorschriften und führt eine Liste der Datensammlungen.
- Der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte** nimmt Aufgaben der Aufsicht und der Beratung bei Privatpersonen und Bundesorganen wahr. Zudem führt er ein Register der Datensammlungen, das über Internet zugänglich ist.
- Der oder die **kantonale** Datenschutzbeauftragte nimmt ähnliche Aufgaben auf Kantonsebene wahr.

Gesetzliche Grundlagen

Dieser Leitfaden stützt sich auf das Bundesgesetz über den Datenschutz (DSG) – insbesondere auf Artikel 7 – und die Verordnung zum Bundesgesetz über den Datenschutz (VDSG) – insbesondere die Artikel 8–11 sowie 20 und 21.

Technische und organisatorische Massnahmen

Die Gefahren, die mit Informationssystemen verbunden sind, lassen sich mit technischen und organisatorischen Massnahmen verringern. So muss ein Informationssystem, das Personendaten enthält, bestimmten Kriterien genügen, um die Sicherheit dieser Daten zu gewährleisten.

Technische Massnahmen hängen direkt mit dem Informationssystem zusammen. Organisatorische Massnahmen hingegen betreffen das Umfeld des Systems, insbesondere die Personen, die es nutzen. Nur ein Zusammenspiel beider Arten von Massnahmen verhindert die Vernichtung oder den Verlust von Daten oder Irrtümer, Fälschungen und unberechtigten Zugang. Diese Massnahmen gehören zum Lebenszyklus eines Informationssystems und müssen auf jeder Stufe des Systems greifen.

Die nachfolgende Abbildung 1 gibt einen Überblick über den Lebenszyklus eines Informationssystems. Sie stellt dar, wie die Daten erfasst, bearbeitet, weitergegeben, aufbewahrt usw. werden und zeigt, auf welchen Stufen Dritte – Mitarbeiterinnen und Mitarbeiter, datenbearbeitende Dritte oder Personen, deren Daten im System enthalten sind – eingreifen können.



Inhalt des Leitfadens

Der Leitfaden orientiert sich an den vier Schwerpunkten, die aus Abbildung 1 abgeleitet werden. Er behandelt technische und organisatorische Massnahmen im Zusammenhang mit dem Zugang zu den Daten (1), dem Lebenszyklus von Daten (2), dem Datenaustausch (3) und mit dem Auskunftsrecht (4).

Jeder Schwerpunkt wird unter verschiedenen Aspekten und mit den dazugehörigen Massnahmen dargestellt. Zu jedem Aspekt werden ein paar bewährte Praktiken angegeben, gleichsam Hilfen für die Entwicklung von Applikationen, die die Privatsphäre respektieren. Selbstverständlich müssen die Massnahmen je nach Sensibilität der Daten, nach Art der Bearbeitung und nach Umfang der benutzten Informationen auf den Einzelfall angepasst werden.

Schliesslich werden bestehende Instrumente dargestellt, die es erlauben, die Risiken aus Sicht des Datenschutzes vorzusehen oder die getroffenen Massnahmen formell zu beschreiben.

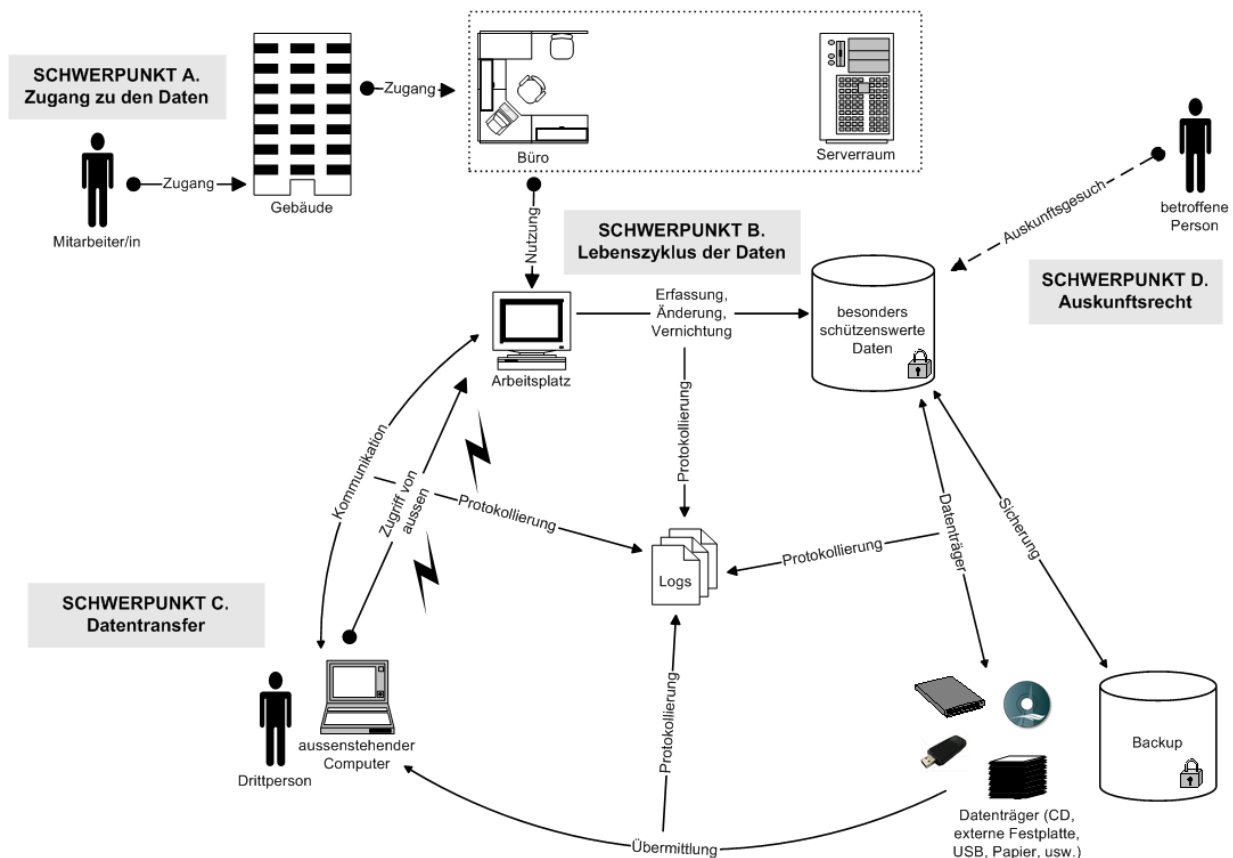


Abbildung 1. Überblick über die technischen und organisatorischen Massnahmen.
Jeder Teil der Abbildung entspricht einem Schwerpunkt des Leitfadens.



SCHWERPUNKT A. ZUGANG ZU DEN DATEN

Der erste Themenkreis ist dem Zugang der verschiedenen Nutzerinnen und Nutzer zu den Daten gewidmet. Dabei zählen verschiedene Blickwinkel. So muss die Frage des physischen Standorts der Daten eingehend geprüft werden: Wo stehen die Datenserver, und wie kann unter Berücksichtigung aller beteiligten Personen deren Sicherheit garantiert werden? Dann muss festgelegt werden, wie die Daten bspw. eingesehen oder geändert werden können. Das bringt unterschiedliche Sicherheitsanforderungen mit sich: Die Computer der Mitarbeiterinnen und Mitarbeiter 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.

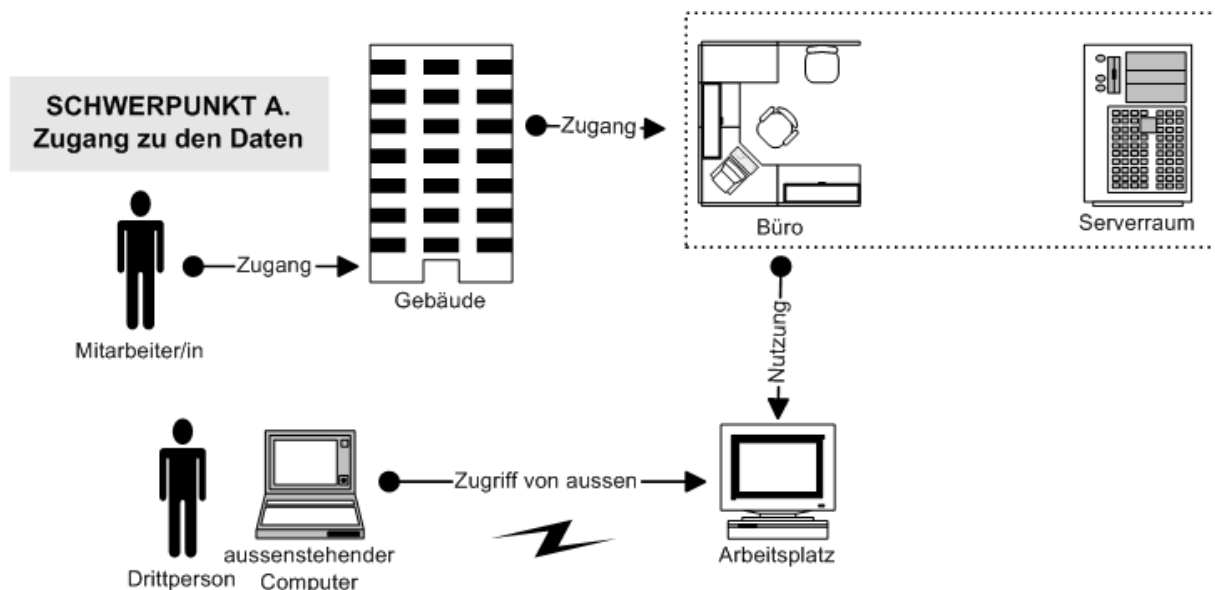


Abbildung A. Zugang zu den Daten

Abbildung A stellt folgende Fragen, die nun eingehend behandelt und zu denen konkrete Massnahmen empfohlen werden.

- A.1 Wie sichert man die Räumlichkeiten?
- A.2 Wie stellt man den Schutz der Server sicher?
- A.3 Wie können die Arbeitsplätze geschützt werden?



A.4 Wie stellt man sicher, dass die Benutzerinnen und Benutzer identifiziert und authentifiziert werden?

A.5 Wie soll der Zugang zu den Benutzerdaten geschützt werden?

A.6 Wie lässt sich der Online-Zugang kontrollieren?

A.1 Sicherheit der Räumlichkeiten

Als Räumlichkeiten gelten die Büros derjenigen Personen, die das System benutzen und somit auch Zugang zu den Daten haben (zur Datenaufbewahrung in den Serverräumen siehe Abschnitt A.2). Die PCs sind die peripheren Geräte, über die auf die Daten zugegriffen werden kann. Daher muss der Zugang zu diesen Geräten kontrolliert werden. Nur berechnete 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 Mitarbeiterinnen und Mitarbeiter 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 sicher nicht 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; die Verantwortung bleibt aber beim Auftraggeber.

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.



A.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.

A.3 Sicherheit des Arbeitsplatzes

Die Mitarbeiterinnen und Mitarbeiter bearbeiten die Daten auf ihren PCs 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 mit einem Passwort zu schützen, das nur die betreffende Mitarbeiterin 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.



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 Mitarbeiterinnen und Mitarbeiter nehmen können.
- Gedruckte Dokumente liegen nicht unbeaufsichtigt beim Drucker herum. Dazu gibt die Mitarbeiterin oder der Mitarbeiter beispielsweise einen Code in den Drucker ein, der seinen Druckauftrag auslöst.
- Die Mitarbeiterinnen und Mitarbeiter 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.

A.4 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. ein Badge), 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, wenn mindestens zwei dieser Möglichkeiten zusammen benutzt werden müssen (z.B. Badge und Passwort).

Die Authentifizierung braucht es also, damit die Benutzerinnen und Benutzer die Räumlichkeiten betreten können und über den Computer Zugang zu den Daten erhalten. Die Identifizierung hingegen erlaubt es nachzuvollziehen, wer zu einem bestimmten Zeitpunkt welche Daten im System erfasst, geändert oder vernichtet hat.

Mit der Methode der einmaligen Authentifizierung (Single Sign-On, SSO) können die Benutzerinnen und Benutzer auf verschiedene Anwendungen zugreifen und müssen sich dafür nur einmal authentifizieren (lassen).



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 einen Badge 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.
- Das Passwort muss stark sein und regelmässig gewechselt werden. Ein starkes Passwort enthält mindestens 8 Zeichen, und zwar grosse und kleine Buchstaben, Ziffern und Sonderzeichen.
- 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.¹

A.5 Zugang zu den Daten

Die Daten werden in zentralen Servern gelagert. Die meisten Mitarbeiterinnen und Mitarbeiter brauchen nicht den 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.

¹ www.derbeauftragte.ch > Themen > Datenschutz > Biometrie



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 Mitarbeiterin oder der Mitarbeiter authentifiziert sich beim Anschalten des Systems. Je sensibler die Daten, die sie oder er bearbeitet, desto höher sind die Anforderungen an die Authentifizierung.
- Der Zugang zu den Daten des Systems wird nach den Regeln des Abschnitts B.2 protokolliert.

A.6 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 kann ein Mitarbeiter um einen solchen Zugang ersuchen, weil er ausserhalb arbeiten und von dort auf seinen 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 Subunternehmen Zugang zu den Daten verlangen. Dieser Fall muss klar mit einer starken Authentifizierung geregelt werden. Missbräuchliche Zugriffe müssen unbedingt verhindert werden.

Abschnitt C.1 (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 von Abschnitt C.2 (Protokollierung) protokolliert werden.



SCHWERPUNKT B. LEBENSZYKLUS VON 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) sicher ist. Nun geht es darum, diese Sicherheit während dem ganzen Lebenszyklus der Daten zu gewährleisten. Die Daten müssen vom Moment ihrer Einspeisung in das 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 in 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 Probleme 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.

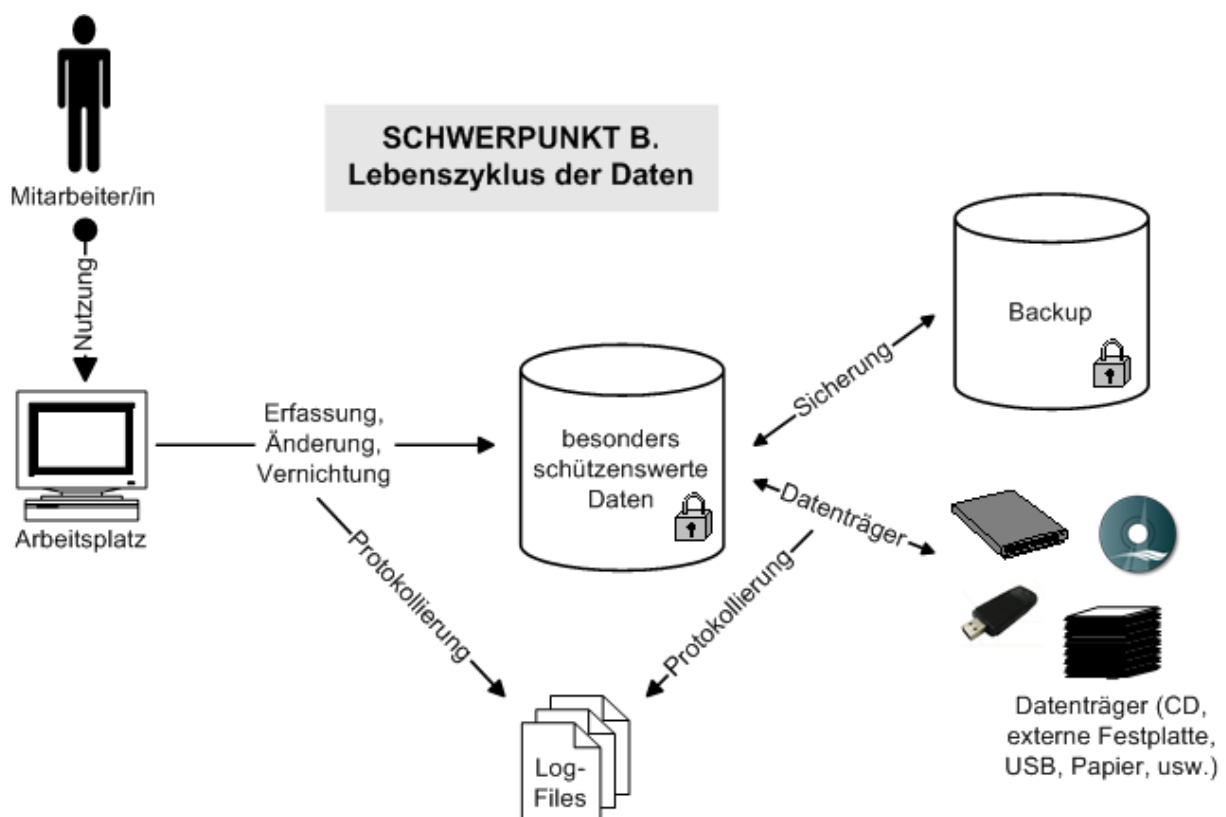


Abbildung B. Lebenszyklus der Daten



Zu diesem Schwerpunkt behandeln wir folgende in Abbildung B illustrierten Fragen:

- B.1 Wie organisiert man die Erfassung der Daten ins System?
- B.2 Wie soll die Datenbearbeitung überwacht werden (Protokollierung)?
- B.3 Wie werden die Daten pseudonymisiert oder anonymisiert?
- B.4 Wie werden die Daten verschlüsselt?
- B.5 Wie lässt sich die Sicherheit der verschiedenen Datenträger gewährleisten?
- B.6 Wie werden die Daten sicher aufbewahrt?
- B.7 Wie lassen sich Daten endgültig vernichten?
- B.8 Wie werden ausgelagerte Projektarbeiten behandelt?
- B.9 Wie geht man mit der Informationssicherheit und dem Datenschutz um?

B.1 Datenerfassung

Ein erster heikler Punkt ist die Erfassung der Daten – es gilt, unter allen Umständen zu verhindern, dass unvollständige oder falsche Daten erfasst werden. Denn bei späteren Bearbeitungen kann sich daraus ein falsches Bild ergeben, was wiederum zu Fehlentscheidungen führen kann. Es ist deshalb wichtig, Mechanismen zu entwickeln, die zur Minimierung der Fehlergefahr bei der Datenerfassung durch die Mitarbeiterinnen und Mitarbeiter beitragen. Zudem muss man klar unterscheiden, ob unechte Daten in einem System erfasst werden, das gerade getestet wird, oder ob es sich um reale Daten handelt.

Massnahmen

- Die Daten werden nur von dazu ausgebildeten und berechtigten Personen erfasst.
- Im System werden Hilfsmechanismen errichtet. Das System erkennt Informationslücken und führt allenfalls auf den erfassten Daten Wahrscheinlichkeitstests durch.
- In einem Test werden nur Daten verwendet, die entweder fiktiv oder anonymisiert sind.
- Eine Protokollierung nach den Regeln von Abschnitt B.2 ist möglich.

B.2 Protokollierung

Es kann von grossem Nutzen sein zu wissen, welche Bearbeitungen mit welchen Daten vorgenommen worden sind, egal, ob es sich dabei um die Erfassung neuer oder die Änderung oder Vernichtung bestehender Daten handelt. Wenn ein Problem auftaucht, erlauben solche Aufzeichnungen herauszufinden, wo ein Zwischenfall, ein unbefugter Zugriff oder eine unbefugte Bearbeitung von Daten stattgefunden hat. Die einzelnen Handlungen können protokolliert werden; alle Ereignisse im Zusammenhang mit dem Informationssystem werden sequentiell aufgezeichnet. Die Aufbewahrungszeit dieser «Logfiles» (Protokolle) bestimmt sich nach der Sensibilität der Daten: je sensibler die Daten, desto länger wird die Aufbewahrungszeit.



Der Zugriff auf die Daten, die Erfassung neuer oder die Änderung oder Vernichtung bestehender Daten etc. – alle diese Vorgänge können protokolliert werden. Obligatorisch ist die Protokollierung aber nur, wenn besonders schützenswerte Daten bearbeitet werden und die Präventionsmassnahmen für die Gewährleistung der Datensicherheit nicht ausreichen.

Auch in den anderen Fällen kann ein Protokollierungsmechanismus ins System integriert werden. Die Protokollierung muss aber klar notwendig sein und präzise umschriebenen Zwecken dienen. Die Menge protokollierter Informationen und die Aufbewahrungsdauer für die Logfiles müssen verhältnismässig sein.

Massnahmen

- Für die Einrichtung eines Protokollierungsmechanismus ist ein Katalog mit klar umschriebenen Kriterien zu erstellen.
- Inhalt und Aufbewahrungsdauer der Logfiles stehen in einem Verhältnis zu den Daten und den vorgenommenen Bearbeitungen.
- Die Mitarbeiterinnen und Mitarbeiter 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.
- Der Protokollierungsmechanismus wird gegen allfällige Attacken und unbefugte Zugriffe, deren Ziel die Veränderung der Protokollinhalte ist, geschützt.

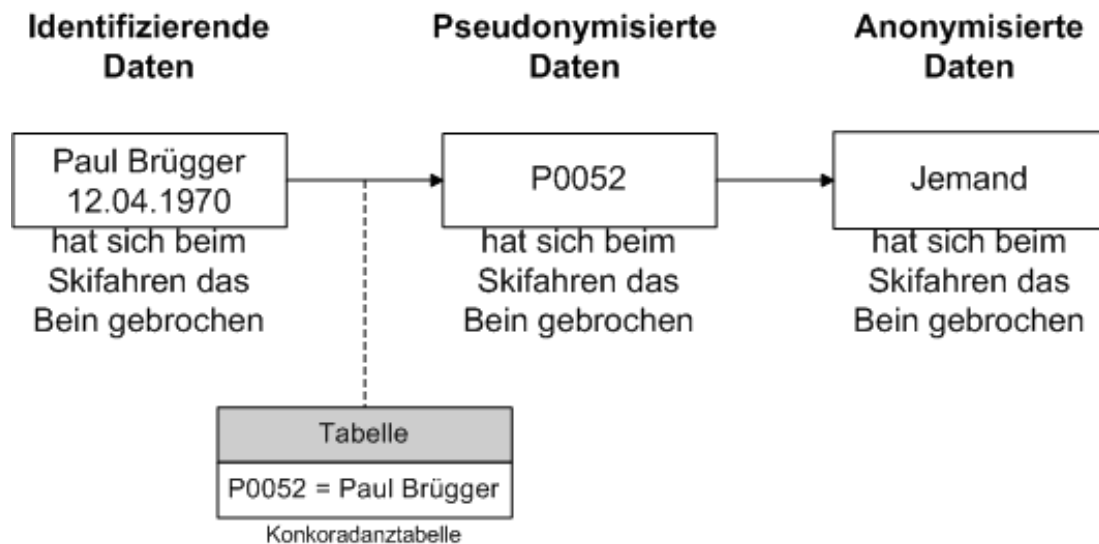
B.3 Pseudonymisierung und Anonymisierung

Damit die Personen, deren Daten in einem System bearbeitet werden, nicht identifiziert werden können, müssen die Daten pseudonymisiert oder anonymisiert werden. Bei der Pseudonymisierung werden alle Daten, die Rückschlüsse auf eine konkrete Person zulassen, durch neutrale Angaben (Pseudonym) ersetzt. Eine Konkordanztabelle hält fest, welches Pseudonym welchen identifizierenden Daten entspricht. Solange diese Tabelle besteht und zugänglich ist, kann die Pseudonymisierung rückgängig gemacht werden.

Bei der Anonymisierung hingegen werden die Daten selber und alle Möglichkeiten, die Originaldaten wieder zu erlangen, definitiv beseitigt. Die Person lässt sich nicht mehr identifizieren, und der Vorgang ist irreversibel. Vollkommen anonymisierte Daten gelten daher nicht mehr als Personendaten.



Folgende Abbildung stellt diesen Prozess dar:



Massnahmen

- Wenn es der Zweck des Projekts zulässt, sollten vorzugsweise anonymisierte Daten verwendet werden. Anonymisierte Daten fallen nicht mehr unter das Bundesgesetz über den Datenschutz, und die meisten in diesem Leitfaden dargestellten Massnahmen erübrigen sich.
- Sowohl bei der Pseudonymisierung als auch bei der Anonymisierung darf keine indirekt identifizierende Information bearbeitet werden. Eine indirekt identifizierende Information erhält man, wenn verschiedene Informationen, die je einzeln keine Rückschlüsse auf die Person zulassen, zusammen aber Aufschluss über die Identität der Person geben.
- Wenn die Anonymisierung nicht möglich ist, arbeiten die Mitarbeiterinnen und Mitarbeiter möglichst mit pseudonymisierten Daten.
- Die Konkordanztable muss gesichert werden. Sie darf nur für eine beschränkte Zahl von Mitarbeiterinnen und Mitarbeitern zugänglich sein. Wenn möglich ist sie zu verschlüsseln.
- Wenn die Pseudonymisierung nicht möglich ist, arbeiten die Mitarbeiterinnen und Mitarbeiter mit personenbezogenen Daten. Sind diese besonders schützenswert, müssen sie verschlüsselt gespeichert werden. (vgl. Abschnitt B.4 Verschlüsselung).



B.4 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.

Der nächste Schwerpunkt (C. Datenaustausch) behandelt die Probleme rund um den Datenaustausch. Damit verbundene Gefahren können durch angemessene Verschlüsselung verringert werden.

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 Mitarbeiterinnen und Mitarbeiter hat Zugang zu den Schlüsseln.

B.5 Sicherheit der Datenträger

Die Daten werden nicht nur auf zentralen Servern und PCs gespeichert; zahlreiche externe Speichermedien ermöglichen den Transfer von Informationen unter Mitarbeitern 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 Mitarbeiterinnen und Mitarbeiter 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.

B.6 Datensicherung

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

Massnahmen

- Es wird eine Sicherungsstrategie festgelegt, die auf die Daten und ihre Menge und Änderungshäufigkeit abstellt.
- Die Mitarbeiterinnen und Mitarbeiter 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.

B.7 Datenvernichtung

Personendaten sind nicht dafür da, auf unbeschränkte Zeit aufbewahrt zu werden. Die Aufbewahrungsdauer muss festgelegt und Mechanismen zur endgültigen Vernichtung müssen vorgesehen werden. Die Daten auf der Festplatte löschen reicht nämlich nicht aus; sie dürfen nie mehr zugänglich sein. Das Gleiche gilt für Daten auf Papier oder auf mobilen Datenträgern. Auch die Sicherungskopien sind zu vernichten.

Massnahmen

- Daten auf Papier werden mit dem Aktenvernichter vernichtet.
- CD-ROM und andere mobile Datenträger werden ebenfalls physisch vernichtet.



- Daten auf wiederbeschreibbaren Datenträgern werden mit Spezialprogrammen physisch und endgültig gelöscht.

B.8 Auslagerung von Arbeiten (Bearbeitung durch Dritte)

Regelmässig kommt es vor, dass eine Organisation einen Teil ihrer Arbeiten an Drittunternehmen auslagert, bspw. die Entwicklung eines Projekts, der Betrieb eines Systems oder die Datensicherung. Die beauftragende Organisation muss sich vergewissern, dass das beauftragte Unternehmen bezüglich Datenschutz die gleichen Regeln befolgt wie sie selber. Als Auftraggeberin haftet sie für ihre Daten.

Massnahmen

- Im Vertrag mit dem Auftragnehmer wird festgehalten, dass er die Regeln der Auftraggeberin einhalten muss.
- Die Auftraggeberin überprüft regelmässig, ob die Bedingungen des Datenschutzes eingehalten werden.
- Die Übermittlung von Daten zwischen Auftraggeberin und Auftragnehmer wird geregelt.

B.9 Sicherheit und Schutz

Um die Daten optimal zu schützen, muss die Art der Personendaten (nicht-sensible, "sensible" oder hochsensible, nach Definition in der Einleitung) nach Risikostufe (gering, mittel, hoch, sehr hoch) in Beziehung gesetzt werden zur Klassifizierung der Information (INTERN, VERTRAULICH, GEHEIM). So kann eine Matrix nach folgendem Muster erstellt werden, auf deren Grundlage sich der Schutzbedarf angemessen zu den beiden Klassifizierungsskalen festlegen lässt. Die am wenigsten einschneidende Massnahme gilt für alle höheren Stufen.



Datenschutz Infoschutz	nicht- personenbez. Daten	"nicht-sensible" Personendaten	"sensible" Personendaten	"hochsensibel" Personendaten
	Risiko:	gering/mittel	hoch	sehr hoch
nicht-klassif. 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.

Massnahmen

- Das System wird anhand der in der Matrix dargestellten Kriterien erarbeitet.
- Aufgrund der Matrix werden entsprechende Massnahmen ergriffen.



SCHWERPUNKT C. DATENAUSTAUSCH

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.

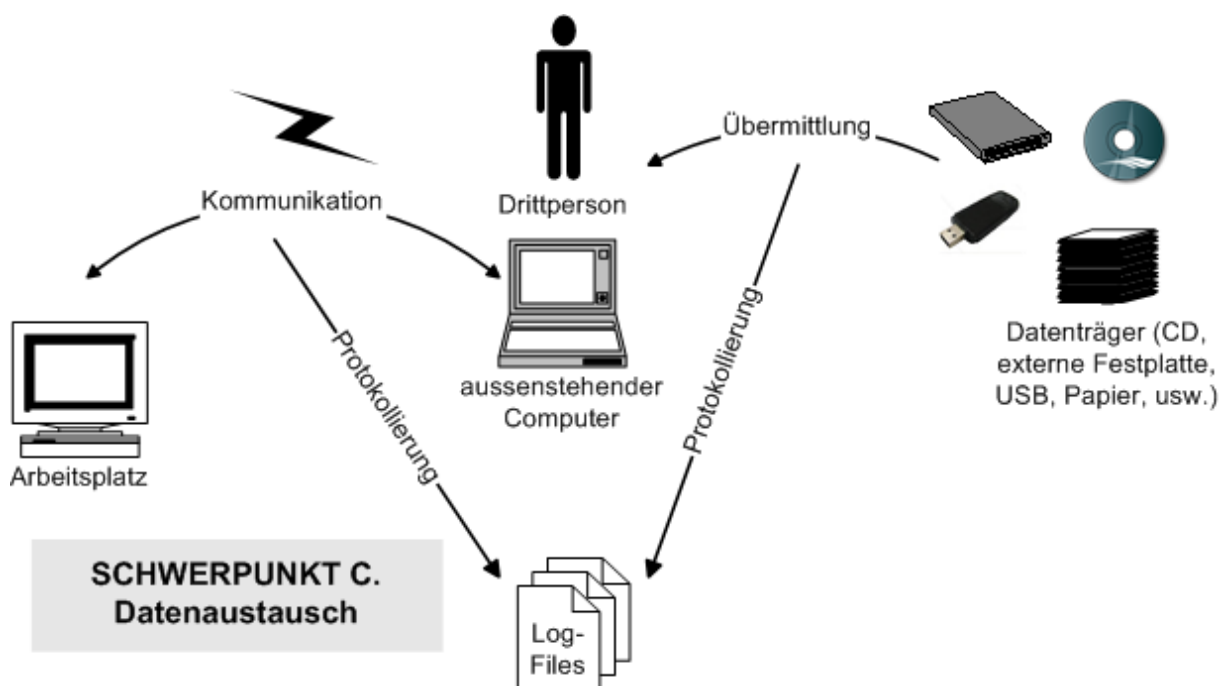


Abbildung C. Datenaustausch

Zu diesem Schwerpunkt behandeln wir folgende in Abbildung C illustrierten Fragen:

- C.1 Wie lässt sich die Sicherheit garantieren?
- C.2 Wie ist eine Mitteilung zu verschlüsseln, die einer aussen stehenden Drittperson übermittelt wird?
- C.3 Wie ist eine Mitteilung zu unterzeichnen, die einer aussen stehenden Drittperson übermittelt wird?
- C.4 Wie können mobile Datenträger sicher weitergegeben werden?
- C.5 Wie die verschiedenen Informationstransfers protokollieren?



C.1 Netzsicherheit

Die Datentransfers in den internen Netzwerken einer Organisation sind zahlreich. So kann es Mitarbeiterinnen und Mitarbeiter 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 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.
- Es ist zu prüfen, ob angesichts der Daten, die zu bearbeiten sind, nicht ein gesichertes Übertragungsprotokoll (TLS) eingesetzt werden sollte.
- Müssen Mitarbeiterinnen und Mitarbeiter oder Dritte von ausserhalb der Organisation auf das Intranet der Organisation zugreifen, muss ein VPN eingerichtet werden.

C.2 Verschlüsselung von Mitteilungen

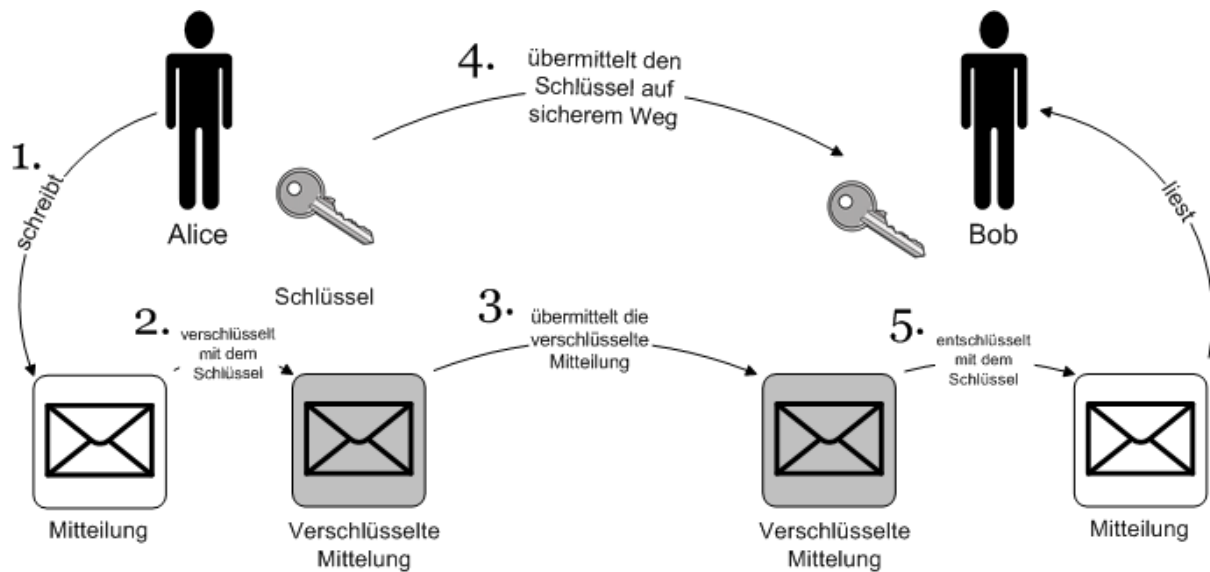
Neben der Festplatte und den Dateien sind gleichzeitig auch die Mitteilungen zu verschlüsseln. Nur so lässt sich ein unerwünschter Zugriff auf die Daten verhindern und vermeiden, dass unberechtigte Dritte eine Mitteilung lesen, verändern oder löschen können.

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



Die symmetrische Verschlüsselung funktioniert nach unten stehendem 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.



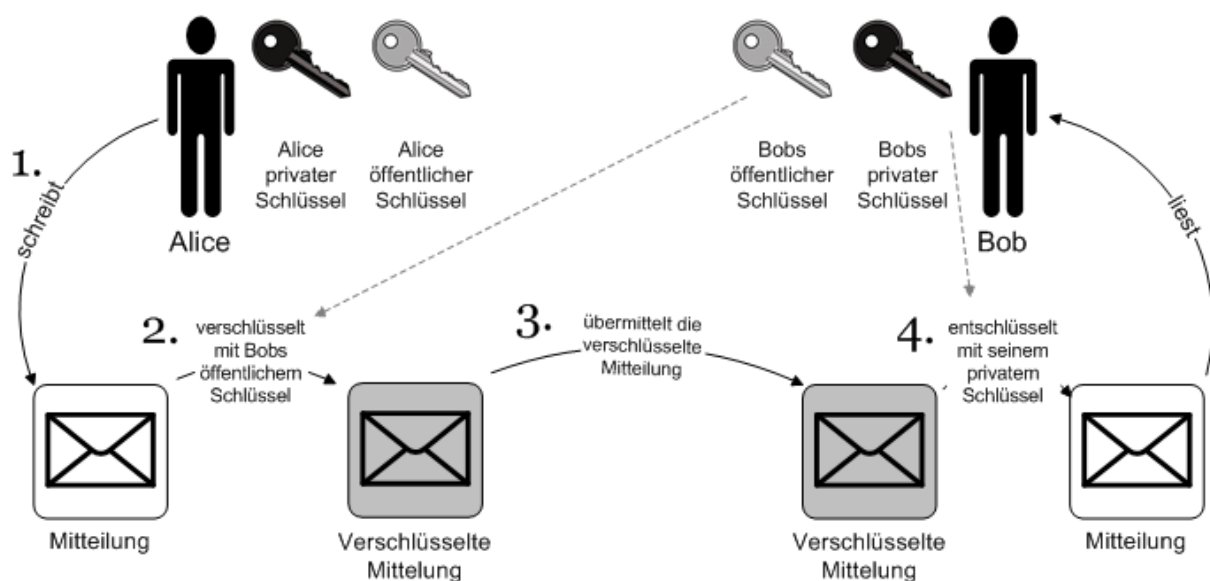
Die symmetrische Chiffrierung lässt sich einfach umsetzen, weil es nur einen Schlüssel dazu braucht. Allerdings ist darauf zu achten, dass dieser Schlüssel auf sichere Art und Weise übergeben wird.

Die asymmetrische Verschlüsselung ist komplexer. 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 C.3 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.



Massnahmen

- Es gilt zu entscheiden, welche Art von Verschlüsselung die geeignete ist. Zu berücksichtigen sind dabei die Sensibilität der Daten und die Drittpersonen, mit denen die Organisation zu tun hat.
- Wird die symmetrische Chiffrierung 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 C.3 Unterzeichnen von Mitteilungen).

C.3 Unterzeichnen von Mitteilungen

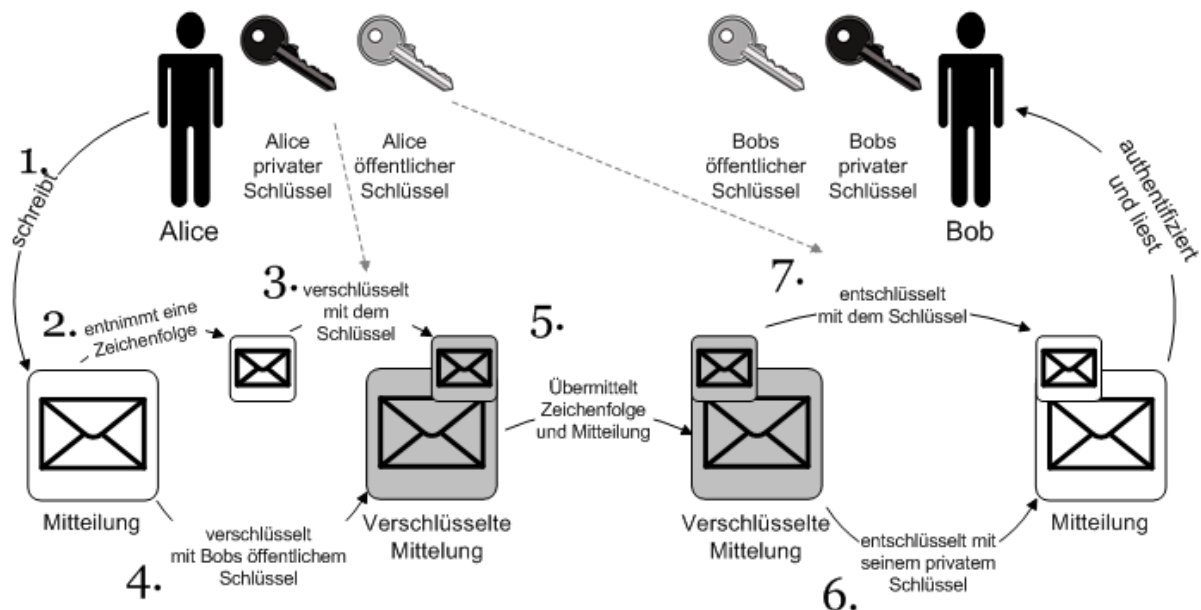
Die Verschlüsselung einer Mitteilung (vgl. Abschnitt C.2 Verschlüsselung von Mitteilungen) stellt sicher, dass nur die Person die Mitteilung lesen kann, die den für die Dechiffrierung



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 Unterschrift auf der Mitteilung kann die Absenderin diese Information sicher übermitteln.

Die 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 Alice' öffentlichem Schlüssel und versichert sich damit, dass sie es war, die ihm die Mitteilung zugestellt hat.



Massnahme

- Die Mitarbeiterinnen und Mitarbeiter werden für die Situationen sensibilisiert, in denen sie ihre Informationen unterzeichnen und verschlüsseln müssen.
- Die Mitarbeiterinnen und Mitarbeiter wissen, wie Mitteilungen verschlüsselt und unterzeichnet werden.



C.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 Trägers 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 vonstatten gehen. So können die Person, die die Daten übergibt, und ihr Empfänger für den Zugang zu den Daten ihre Passwörter kombinieren.

C.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, bei einer falschen Verwendung oder einer Fehlmanipulation können dadurch eine bestimmte Menge von Daten wiedergefunden und der Weg, den die Daten von der Übergabe bis zum Eintreten des Problems zurückgelegt haben, nachvollzogen werden.

Die Anforderungen nach Abschnitt B.2 – Protokollierung gelten auch für die Protokollierung des Datenaustauschs.

Massnahmen

- Es muss ganz genau umschrieben werden, 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 Mitarbeiterinnen und Mitarbeitern anvertraut werden.
- Für die Protokollierung gilt das Verhältnismässigkeitsprinzip. Die Protokollierung der Datenaustauschs richtet sich nach Umfang, Dauer usw.

SCHWERPUNKT D. AUSKUNFTSRECHT

Als betroffene Personen gelten diejenigen, deren Personendaten im System sind. Jede und jeder hat das Recht zu wissen, ob und welche Personendaten über sie oder ihn persönlich vorhanden sind. Existieren solche Daten, kann die betroffene Person die Vernichtung verlangen, sind sie falsch, ihre Berichtigung.



Abbildung D. Auskunftsrecht

Zu diesem Schwerpunkt behandeln wir folgende in Abbildung D illustrierten Fragen:

- D.1 Wie lässt sich gewährleisten, dass die betroffenen Personen ihr Recht geltend machen können?
- D.2 Wie lässt sich garantieren, dass das Verfahren zur Ausübung des Auskunftsrechts immer gleich abläuft (Reproduzierbarkeit des Verfahrens)?

D.1 Recht der betroffenen Personen

Die betroffenen Personen haben das Recht auf Auskunft über ihre Daten. Sie können deren Berichtigung, Sperrung oder Vernichtung verlangen. Die Organisation muss in der Lage sein, solche Gesuche angemessen zu behandeln und im System umzusetzen. Dazu ist ein effizienter Mechanismus zur Suche der Personendaten nötig, und die Operationen müssen erfolgreich durchgeführt werden können. Wenn beispielsweise eine Person die Vernichtung ihrer Daten verlangt, muss das System gewährleisten, dass die Gesamtheit der Daten auch wirklich gelöscht wird.



Massnahmen

- Für die betroffenen Personen steht eine klare Information zur Verfügung. Sie zeigt auf, welche Rechte sie haben.
- Ein Verfahren für die Auskunftsgesuche wird eingerichtet und den Mitarbeiterinnen und Mitarbeitern bekannt gemacht.
- Das System ist mit einem vertrauenswürdigen Suchmechanismus ausgestattet.
- Die Verfahren zur Änderung, Berichtigung, Sperrung und Vernichtung der Daten sind vertrauenswürdig und werden dokumentiert.
- Jede Bearbeitung wird protokolliert.

D.2 Reproduzierbarkeit der Verfahren

Das Verfahren, nach dem Auskunftsgesuche von betroffenen Personen behandelt werden, muss klar festgelegt und reproduzierbar sein. Wenn der Mechanismus im Datenbearbeitungssystem vorprogrammiert ist, können alle Mitarbeiterinnen und Mitarbeiter auf dieselbe Art und Weise Berichtigungen, Sperrungen oder die Vernichtung von Daten vornehmen. Ein vorprogrammierter Mechanismus ist auch praktisch bei einer Kontrolle durch eine Aufsichtsbehörde, weil er belegt, dass das Auskunftsrecht ausgeübt werden kann.

Massnahmen

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



HILFSMITTEL

Gewisse Hilfsmittel zur Umsetzung der technischen und organisatorischen Massnahmen bestehen bereits.

Evaluationsraster

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt ein Evaluationsraster zur Früherkennung von Datenschutzrisiken zur Verfügung, mit dem sich sehr früh im Erarbeitungsprozess eines Projekts diejenigen Punkte identifizieren lassen, die aus der Sicht des Datenschutzes heikel sind.

Das Evaluationsraster kann auf der [Website des EDÖB](#) (Datenschutz - Handel und Wirtschaft - Unternehmen) abgerufen werden.

Das Bearbeitungsreglement

Das Bearbeitungsreglement ist ein vom schweizerischen Recht vorgesehenes Instrument, in dem die zweckmässigen technischen und organisatorischen Massnahmen festgelegt werden. Mit einem solchen Reglement soll die Transparenz sichergestellt werden, die für die Erarbeitung und die Verwaltung einer Personendatensammlung (Sammlung) notwendig ist. Darin können die Unterlagen, die von den verschiedenen mit dem Projekt betrauten Einheiten erarbeitet werden, zusammengefasst und die Informationen zentralisiert werden. Es stellt somit den Datenschutzverantwortlichen und den Systembetreibern eine vollständige Dokumentation zur Verfügung, die es ihnen ermöglicht, auf die bewährten Praktiken zurückzugreifen und sie anzuwenden.

Das Bearbeitungsreglement muss vom Inhaber oder der Inhaberin der Datensammlung erarbeitet werden.

Inhalt des Reglements

Ist der Inhaber oder die Inhaberin der Datensammlung eine Privatperson, so muss das Bearbeitungsreglement einerseits einen Beschrieb der internen Organisation und der Datenbearbeitungs- und -kontrollverfahren enthalten und andererseits die vollständige Dokumentation über die Planung, die Erarbeitung und den Betrieb der Informatikmittel, das heisst der Software und der Hardware.

Ist der Inhaber der Datensammlung ein Bundesorgan, so wird ein Bearbeitungsreglement nur verlangt, wenn (1) die Sammlung besonders schützenswerte Daten oder Persönlichkeitsprofile enthält, (2) von mehreren Bundesorganen genutzt wird, (3) für Dritte wie Kantone, ausländische Behörden, internationale Organisationen oder Privatpersonen zugänglich und (4) mit anderen Sammlungen verknüpft ist.



Der Inhalt des Bearbeitungsreglements für Bundesorgane ist ganz präzise umschrieben:

1. Die interne Organisation – die vom System getätigten Operationen und die Organisationsstruktur – muss dokumentiert werden. Zu nennen sind insbesondere die verschiedenen Zuständigkeiten (Datenschutz, Inhaber der Datensammlung usw.).
2. Die Unterlagen über Planung, Realisierung und Betrieb der Informatikmittel müssen transparent aufgebaut sein.
3. Eine Übersicht über die technischen und organisatorischen Massnahmen zeigt, welche Massnahmen bereits ergriffen wurden.
4. Die Herkunft der Daten und der Bearbeitungszweck müssen beschrieben werden.
5. Die Meldepflicht ist mit allen erforderlichen Angaben umschrieben.
6. Sämtliche Datenfelder werden festgelegt. Eine Zugangsmatrix zeigt, welche Organisationseinheiten und welche Personen Zugang zu den Daten haben.
7. Die Massnahmen zur Ausübung des Auskunftsrechts werden festgelegt.
8. Die Konfiguration der Informatikmittel erwähnt die gesamte eingesetzte Software und Hardware.

Das Bearbeitungsreglement muss regelmässig aktualisiert und den anderen betroffenen Organen zur Verfügung gestellt werden.

Bei der Erarbeitung eines Bearbeitungsreglements kann das Dokument «Was muss ein Bearbeitungsreglement enthalten» aus der Feder des EDÖB helfen².

SCHLUSSBEMERKUNG

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

Für den Datenschutz verantwortlich ist der Inhaber oder die Inhaberin der Datensammlung. Je früher dieses Thema bei der Erarbeitung eines Projekts angegangen wird, desto besser kann der bzw. die Verantwortliche die damit verbundenen Gefahren minimieren.

² www.derbeauftragte.ch > Dokumentation > Datenschutz > Leitfäden > Technische und organisatorische Massnahmen