

Ausgangslage

Sie sind verantwortlicher Informatikleiter in einer mittleren schweizerischen Krankenkasse. Neben dem Hauptsitz in Zürich betreibt die Krankenkasse insgesamt 12 grosse Filialen, die über ein öffentliches, auf X.25 basierendes Kommunikationsnetz untereinander und mit dem Hauptsitz verbunden sind. Das eigentliche Rechenzentrum steht in Zürich – an den einzelnen Standorten stehen neben den Bildschirmarbeitsplätzen ausschliesslich Drucksysteme.

Entsprechend ihrer Versicherungstätigkeit sammelt und speichert die Krankenkasse über die versicherten Personen auch Informationen, welche gemäss dem Datenschutzgesetz als "besonders schützenswerte Personendaten" einzustufen sind. Bei der Überarbeitung des bestehenden Sicherheitskonzeptes sollen die technischen und organisatorischen Massnahmen, die aus Gründen des Datenschutzes getroffen werden müssen, in einem separaten Kapitel zusammengefasst werden.

Aufgabenstellung

Für die auf der folgenden Seite aufgeführten Kontrollbereiche a bis h gemäss Art. 9 VDSG sind praxisgerechte Massnahmen zu finden, welche die in Art. 8 Abs. 1, 2 und 3 VDSG gestellten Anforderungen berücksichtigen.

Beantworten Sie für Ihre Teilaufgabe (einen der Kontrollbereiche a, b, ... oder h) die nachfolgenden vier Fragen:

- 1 Was ist das Schutzziel in diesem Kontrollbereich? Erläutern Sie falls notwendig die im Gesetzestext verwendeten Begriffe.
- 2 Welche Bedrohungen sollen dadurch abgedeckt werden? Zeigen Sie diese Bedrohungen an zwei bis drei konkreten Beispielen auf (z.B. Lesen "gelöschter Dateien" mit Norton-Utilities).
- 3 Mit welchen Massnahmen kann grundsätzlich das aufgeführte Ziel erreicht werden?
- 4 Welche dieser Massnahmen implementieren Sie aufgrund der geforderten "Angemessenheit"?

Ausschnitt aus der Vollzugsverordnung

4. Abschnitt: Technische und organisatorische Massnahmen**Art. 8 Allgemeine Massnahmen**

- 1 Wer als Privatperson Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten, um einen angemessenen Datenschutz zu gewährleisten. Insbesondere schützt er die Systeme gegen folgende Risiken:
 - a unbefugte oder zufällige Vernichtung;
 - b zufälligen Verlust;
 - c technische Fehler;
 - d Fälschung, Diebstahl oder widerrechtliche Verwendung;
 - e unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.
- 2 Die technischen und organisatorischen Massnahmen müssen verhältnismässig sein. Insbesondere tragen sie folgenden Kriterien Rechnung:
 - a Zweck der Datenbearbeitung;
 - b Art und Umfang der Datenbearbeitung;
 - c Einschätzung der möglichen Risiken für die betroffenen Personen;
 - d gegenwärtiger Stand der Technik.
- 3 Diese Massnahmen sind periodisch zu überprüfen.
- 4 Der Datenschutzbeauftragte kann in diesem Bereich Empfehlungen in Form von Handbüchern erlassen.

Art. 9 Besondere Massnahmen

- 1 Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:
 - a *Zugangskontrolle*: unbefugten Personen ist der Zugang zu den Einrichtungen in denen Personendaten bearbeitet werden, zu verwehren;
 - b *Personendatenträgerkontrolle*: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
 - c *Transportkontrolle*: bei der Bekanntgabe von Personendaten, sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;
 - d *Bekanntgabekontrolle*: Datenempfänger, denen Personendaten durch Einrichtungen zur Datenübertragung bekanntgegeben werden, müssen identifiziert werden können;
 - e *Speicherkontrolle*: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;
 - f *Benutzerkontrolle*: die Benutzung von automatisierten Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;
 - g *Zugriffskontrolle*: der Zugriff der berechtigten Personen ist nur auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
 - h *Eingabekontrolle*: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten, zu welcher Zeit und von welcher Person eingegeben wurden.
- 2 Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.

Risikogerechte Massnahmen gemäss VDSG Art. 9 (Lösungsvorschlag für besonders schützenswerte Personendaten)

Dieser Lösungsvorschlag für besonders schützenswerte Personendaten erhebt keinen Anspruch auf Vollständigkeit. Er enthält zusätzlich zu den von unabhängigen Spezialisten erarbeiteten Massnahmen teilweise auch die später veröffentlichten Vorschläge aus dem Leitfaden des eidg. Datenschutzbeauftragten. Ob eine Massnahme angemessen ist im Sinne von Art. 7 VDSG, lässt sich nur mittels einer sorgfältigen, professionellen Beurteilung sämtlicher relevanter Faktoren bestimmen.

Erläuterung:

- o: generell empfehlenswerte Massnahmen
- + : zusätzliche Massnahmen bei erhöhtem Risiko für die Betroffenen

Zugangskontrolle: Unbefugten Personen ist der Zugang zu denjenigen Einrichtungen zu verwehren, mit denen Personendaten bearbeitet werden (Zentralrechner, Server, Arbeitsplatzrechner, Bildschirme/Terminals, Drucker, Verteilerschränke, Netzwerk-Komponenten, ...). Es geht bei diesem Punkt um den physischen Zugang zu diesen Räumlichkeiten resp. um den physischen Zugriff auf die Daten zum Beispiel bei (manuellen, halb-/vollautomatischen) Ablagesystemen.

- o alle "Einrichtungen" in geschützte Räumlichkeiten stellen, wo nur Berechtigte Zutritt haben
- o Einblick auf Bildschirme für Unberechtigte verunmöglichen (z.B. im Beratungsbereich)
- o "clean-desk" (z.T. "clear desk" genannt) für alle Arbeitsplätze mit Kontakt zu Drittpersonen (Kunden; Drittpersonen sind auch andere Mitarbeiter, welche diese Daten nicht kennen müssen!)
- + Fremdpersonen wie Kunden, Service-, Reparatur- oder Reinigungspersonal in geschützten Räumlichkeiten (Sicherheitszonen) permanent beaufsichtigen
- + Zutrittskontrollsystem zu Räumlichkeiten/Sicherheitszonen; gekoppelt mit Einbruchalarm
- + fälschungssichere Protokollierung sämtlicher Personen-Verschiebungen (Hinein-/Hinausgehen)
- + Arbeitsplatzgeräte (PC, Terminal, Kommunikationsports) mit Schlössern o.Ä. abschliessen
- + Abtrennen der Räumlichkeiten, in denen Benutzer personenbezogene Informationen bearbeiten, von anderen Unternehmensbereichen (dies bedingt oft eine Änderung der Arbeitsabläufe)
- + Neue Anwendungen DSGVO-gerecht entwickeln, so dass eine räumliche Abtrennung möglich ist

Personendatenträgerkontrolle: Es ist zu verhindern, dass unbefugte Personen Datenträger (alle Arten von Medien: Disketten, Tapes, Cartridges, COM-Fichen, Cds, Papier!, usw.) lesen, kopieren, verändern oder entfernen können. Es ist auch zu verunmöglichen, dass Personendaten unkontrolliert auf Datenträger übertragen werden. Achtung: Transportierte Datenträger unterliegen der *Transportkontrolle*; sobald ein Datenträger im automatisierten System eingeschoben ist, gilt er als Datenspeicher und unterliegt der *Speicher-* und auch der *Zugriffskontrolle*.

- o Aufbewahrungsvorschriften für Umgang mit Datenträger erstellen und Einhaltung kontrollieren
- o Datenträger unter Verschluss halten (im RZ in Robotersystemen führen)
- o Datenträger-Inventar mit Zugangs- und Abgangskontrolle führen
- o Ab-/Ausgabe nur an berechtigte Personen mit Begleitpapieren und unter Protokollierung
- o kontrollierte Vernichtung der Datenträger (kontrolliertes Löschen sämtlicher Informationsspuren auf dem Datenträger resp. gesicherte Zerstörung)
- o kontrolliertes Löschen des freien Inhaltes (durch mehrmaliges Überschreiben) von Datenträgern vor ihrer Weitergabe an Dritte
- + Datenträger grundsätzlich und immer verschlüsseln
- + für Datenträger in Rechenzentren Diebstahlschutzvorrichtungen wie in Warenhäusern
- + das Einschieben von Datenträgern nur für berechtigte Personen ermöglichen (Schloss, ...)
- + Verhinderung von Kopier- oder gleichartigen Funktionen oder Befehlen
- + LAN-Arbeitsplätze ohne *externe* Datenträger installieren (Backup auf Fileservern)
- + LAN-Arbeitsplätze auch ohne *interne* Datenträger installieren (Dateien nur auf Fileservern)

Transportkontrolle: Bei der Bekanntgabe von Personendaten (damit ist die Übergabe z.B. beim Terminal oder Drucker an den Empfänger gemeint) sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Der Datenempfänger muss die Gewissheit haben, dass er die Daten in ihrer ursprünglichen Form erhalten hat und kein Dritter die Daten eingesehen oder kopiert hat.

Zu unterscheiden ist dabei zwischen dem *logischen* Transport von Daten (Übermittlung) und dem *physischen* Transport von Datenträgern.

Übermittlung:

- o Verhaltensregeln für Umgang mit Fax, Telex usw. aufstellen (Welche Art Informationen oder Dokumente dürfen an welche Stellen oder Personen verschickt werden?)
- o protokollieren, was an wen versandt wurde
- o bei Übermittlung ins Ausland Leitungen grundsätzlich verschlüsseln
- + alle Leitungen ausserhalb des kontrollierten Bereichs des Unternehmens verschlüsseln (noch besser: alle Leitungen generell verschlüsseln)
- + Meldungen authentisieren (mit Prüfsummen kryptographisch sichern)
- + fälschungssichere Protokollierung der Meldungsinhalte (Nachvollziehbarkeit, Beweisbarkeit)
- + digitale Unterschrift des Absenders über gesamten Meldungsinhalt
- + Informationen aufsplitten auf verschiedene Übertragungen resp. Übertragungswege

Physischer Transport:

- o Verpackungs- und Versandvorschriften (analog Wertsendungen)
- o Informationen aufsplitten auf verschiedene Datenträger und Transportwege
- + Datenträger auf gesamten (physischen) Transport generell verschlüsseln

Die *Bekanntgabekontrolle* soll ermöglichen, dass die Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekanntgegeben werden, identifiziert werden können. Dabei muss auch im nachhinein feststellbar sein, an welche Personen oder Organe Daten übertragen werden bzw. wurden. Es geht also um die Nachvollziehbarkeit (anhand von Protokollen und Dokumentationen), wer wann und zu welchem Zweck welche Informationen erhalten hat. Eine Protokollierung ist nicht zwingend vorgeschrieben solange z.B. die Nachvollziehbarkeit aufgrund der vorhandenen Abläufe möglich ist.

- o Dokumentation des Informationsflusses (wer erhält wann warum welche Daten?)
- o Eingabe/Verifikation der Benutzeridentifikation mit *dynamischen* Passwörtern (sog. Einmal-Passwörter) oder kryptographischen Verfahren
- o Verbindung zum Rechner nach kurzer Dauer ohne Benutzer-Aktivität ausschalten (Timeout)
- o Standby-Funktion implementieren (Benutzer kann Terminal für kurzfristige Absenzen selbständig sichern)
- o Outputverteilung kontrollieren (Bewilligungsverfahren; Funktionentrennung Druck, Versand und Behändigung des Output; Journalisierung)
- o Output kontrolliert vernichten (Shredden oder Verbrennen)
- o kein Download von Daten (Filetransfer) auf PC oder andere Netze
- o keine Heimarbeitsplätze mit Zugriff auf personenbezogene Informationen
- o keine Kopiergeräte im Outputbereich
- + Print-Screen-Funktion unterbinden
- + Authentisierung der Benutzeridentität in kurzen Abständen (maschinell unterstützt) wiederholen
- + Versand von Post mittels Fensterkouverts (verhindert bei Verpackungsfehlern einzelner Seiten Versand an falsche Empfänger).

Mit Hilfe der *Speicherkontrolle* soll verhindert werden, dass unbefugte Eingaben in den Speicher (Datensammlungen oder Programme!) sowie unbefugte Einsichtnahmen, Veränderungen oder Löschungen gespeicherter Personendaten vorgenommen werden können. Unter Speicher werden dabei einerseits Arbeitsspeicher (RAM, ROM, I/O-Buffer) und andererseits Datenträger verstanden, sofern sich diese *im* System befinden (z.B. eine ins Laufwerk eingelegte Diskette; eine eingebaute Harddisk, eine eingelegte Wechselplatte). Die Speicherkontrolle deckt somit vor allem systemnahe Bedrohungen ab. Zahlreiche Massnahmen sind in guten Betriebssystemen bereits implementiert (z.B. Verhinderung, dass anderer Prozess auf den eigenen Speicherbereich zugreifen kann, oder, dass ein abstürzendes Programm das gesamte System lahmlegt).

- o Starkes Zugriffsschutzsysteme implementieren und Installation regelmässig überprüfen
- o Berechtigungen für Dienstprogramme (Utilities) nach dem "need-to-know-Prinzip" vergeben
- o keine datenmanipulierenden Hilfsprogramme ("Flick-Werkzeuge", Editor, Compiler, ...) im Produktionsbereich
- o produktive Daten von Entwicklungsumgebung abschotten (keine Tests mit echten Daten)
- o sauberes Changemanagement für Programmänderungen inklusive restriktiv angewandter Zügelverfahren von der Test- in die Produktionsumgebung
- o Wartung durch Externe sorgfältig überwachen
- o Fernwartung (über Netzwerk) sorgfältig überwachen oder grundsätzlich verbieten
- + vor Fernwartungsdurchführung Datenbestände *physisch* abkoppeln
- + keine Query-Abfragemöglichkeiten auf sensitiven Datenbeständen
- + keine Fernsteuerung der Rechner (Stichwort: "unbedientes Rechenzentrum")
- + zertifiziertes Betriebssystem installieren
- + regelmässige und automatische Auswertung von Überwachungsprotokollen
- + Daten grundsätzlich verschlüsselt speichern

Mit Hilfe der *Benutzerkontrolle* will man erreichen, dass automatisierte Datenverarbeitungssysteme mittels Einrichtungen zur Datenübertragung (Kommunikationseinrichtungen) nur durch befugte Personen benutzt werden können. Es geht also um den Zugriff auf die Systeme mittels Netzwerken.

- o Kommunikationsnetz von Aussenwelt isolieren (Firewalls mit Filterung der Meldungsinhalte)
- o Wählleitungsanschlüsse resp. Kommunikationsnetz sehr sorgfältig überwachen
- o Authentisierung des Benutzers mit dynamischen Passwörtern oder kryptographischen Verfahren
- o Zugriffsschutzsystem mit starken Mechanismen implementieren
- o keine Mailboxen auf dem System installieren
- + zeitliche Einschränkungen auf Netzwerkebene
- + Zugriff nur von bestimmten Standorten (sofern technisch möglich)
- + Call-Back oder geschlossene Benutzergruppen (z.B. in X.25: closed user group)
- + sämtliche Meldungen mit kryptographischen Mechanismen vor Verfälschung usw. sichern
- + den gesamten Meldungsverkehr grundsätzlich verschlüsseln (verhindert, dass erfolgreiche Hacker eine Verbindung zum System aufbauen können)

Die *Zugriffskontrolle* soll gewährleisten, dass auch Berechtigte nur auf diejenigen Personendaten Zugriff haben, die sie für die Aufgabenerfüllung benötigen. Der Inhaber der Datensammlung ist verpflichtet, die Zugriffsbewilligung so zu erteilen, dass Art und Umfang der Datenbearbeitung auf den jeweiligen Aufgabenträger abgestimmt ist.

- o Zugriffsschutzsystem mit starken Mechanismen implementieren
- o strikte Anwendung des "need-to-know"-Prinzips bei Vergabe von Berechtigungen
- o periodischer Vergleich zwischen erteilten und effektiv benötigten Berechtigungen
- o Verantwortliche (Owner) bestimmen, die Berechtigungen vergeben und überwachen
- o versuchte/erfolgte Zugriffe protokollieren und nach "verdächtigen Ausnahmen" auswerten
- + Schreibberechtigungen restriktiv erteilen

Die *Eingabekontrolle* soll gewährleisten, dass in automatisierten Systemen nachträglich geprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden. Die Nachvollziehbarkeit muss nicht zwingend durch Protokollierung gewährleistet werden. Anhand von Belegen muss es aber möglich sein, die jeweiligen Eingaben ins System nachvollziehen zu können.

- o Richtige und vollständige Eingabe der Erfassungsbelege
- o Protokollierung und Auswertung der Eingaben
- o Aufbewahrung der Protokolle über viele Jahre (über vorgesehene Frist von einem Jahr hinweg)
- + Anhängen von Mutationsdatum, Zeit und Benutzeridentifikation an alle neu eingegebenen oder veränderten Felder
- + Sammeln der Mutationshistory über viele Jahre resp. gesamte Objekt-Lebenszeit

Generelle Massnahmen

- o Richtlinien für Umgang mit Personendaten entwickeln und durchsetzen
- o Benutzer im Umgang mit personenbezogenen Informationen schulen (z.B. Sorgfaltspflicht, Erteilung von Auskünften usw.)
- o Benutzer müssen ein Merkblatt zum Umgang mit personenbezogenen Informationen unterschreiben (persönliche Übergabe durch Vorgesetzte)
- o Owner für alle personenbezogenen Datensammlungen definieren (mit allen Pflichten des Eigentümer-Prinzips)

Wichtiger Hinweise:

Die vorliegende Fallstudie deckt nicht sämtliche Anforderungen im Bereich der Informatik ab, die durch das Datenschutzgesetz gestellt werden sondern ausdrücklich nur diejenigen der VDSG Art. 8 und 9. Andere Anforderungen sind z.B. die Auskunftspflicht (bedingt entsprechende Suchalgorithmen), das Bearbeitungsreglement (Dokumentation von technischen/organisatorischen Abläufen), Verhinderung der Bekanntgabe ins Ausland resp. der Bearbeitung im Ausland.

Die in VDSG Art. 8 geforderten Massnahmen zur Aufrechterhaltung der Verfügbarkeit (z.B. Clustering der Systeme, Mirroring oder RAID, Backup und Recovery, Notfallkonzepte) sind in der vorliegenden Musterlösung ebenfalls nur ausschnittsweise aufgeführt.

Datenschutzgesetz & Informationssicherheit

Datenschutz

Schutz von personenbezogenen Informationen (Angaben über eine natürliche oder juristische Person) vor Missbrauch, unberechtigter Einsicht oder Verfälschung und damit Schutz des Betroffenen vor Verletzung seiner Privatsphäre.

Personendaten

Angaben über eine natürliche oder juristische Person

besonders schützenswerte Personenendaten

- Gesundheit, Intimsphäre, Rassenzugehörigkeit
- religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten und Tätigkeiten
- Massnahmen der sozialen Hilfe
- Administrative oder strafrechtliche Verfolgung und Sanktionen

Persönlichkeitsprofile

Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben

Wichtige Elemente des Datenschutzgesetzes

- *rechtmässige Beschaffung*: in einer Art und Weise, mit der die betroffene Person rechnen musste. Verboten sind Täuschung, Drohung oder geheime Beschaffung.
- Bearbeitung nur für angegebenen Zweck
- Daten müssen richtig und vollständig sein
- *jederzeit Recht auf Auskunft*: allenfalls mit Kostenbeteiligung (max. Fr. 100.--) nur wenige Einschränkungen bei Vorliegen einer gesetzlichen Grundlage und überwiegendem Interesse Dritter oder überwiegendem öffentlichen Interesse
- *Schutz vor Persönlichkeitsverletzungen*: unrechtmässige Beschaffung, Zweckänderung, Bearbeitung unrichtiger Daten, Bekanntgabe ins Ausland, ungenügende Datensicherheit, Bearbeitung gegen den Willen der Betroffenen, unberechtigte Weitergabe besonders schützenswerten Daten resp. Pers.profilen
- *Datenbearbeitung durch Dritte*: entbindet den Auftraggeber nicht von seiner Verantwortung für die Einhaltung der Datenschutzbestimmungen



Falls in einem Datenbestand gezielt und mit einem vernünftigen Aufwand Informationen zu resp. über eine bestimmte Person gesucht werden können, handelt es sich um eine Datensammlung im Sinne des Gesetzes.

Die aufgeführten Artikel stellen einen Ausschnitt aus der Vollzugsverordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 dar und erheben weder einen Anspruch auf Vollständigkeit noch auf Richtigkeit.

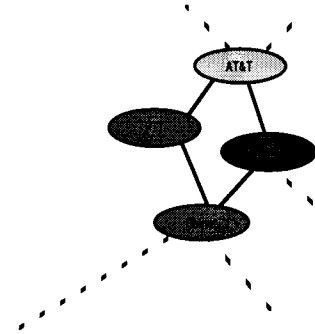
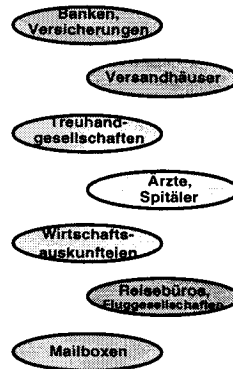
4. Abschnitt: Technische und organisatorische Massnahmen

Art. 8 Allgemeine Massnahmen

Absatz 1

Wer als Privatperson

- Personendaten bearbeitet oder
 - ein Datenkommunikationsnetz zur Verfügung stellt,
- ... gewährleistet einen angemessenen Datenschutz.



... sorgt für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten. Insbesondere schützt er die Systeme gegen folgende Risiken:

Risiken	Vertraulichkeit	Verfügbarkeit	Richtigkeit
a: unbefugte oder zufällige Vernichtung		X	
b: zufälligen Verlust		X	
c: technische Fehler	X	X	X
d: Fälschung, Diebstahl oder widerrechtliche Verwendung	X	(X)	X
e: unbefugtes Ändern, Kopieren, Zugreifen oder andere Bearbeitungen	X		X

2 Die technischen und organisatorischen Massnahmen müssen verhältnismässig sein. Insbesondere tragen sie folgenden Kriterien Rechnung:

- Zweck der Datenbearbeitung;
- Art und Umfang der Datenbearbeitung;
- Einschätzung der möglichen Risiken für die betroffenen Personen;
- gegenwärtiger Stand der Technik.

3 Diese Massnahmen sind periodisch zu überprüfen.

4 Der Datenschutzbeauftragte kann in diesem Bereich Empfehlungen in Form von Handbüchern erlassen.

Art. 9 Besondere Massnahmen

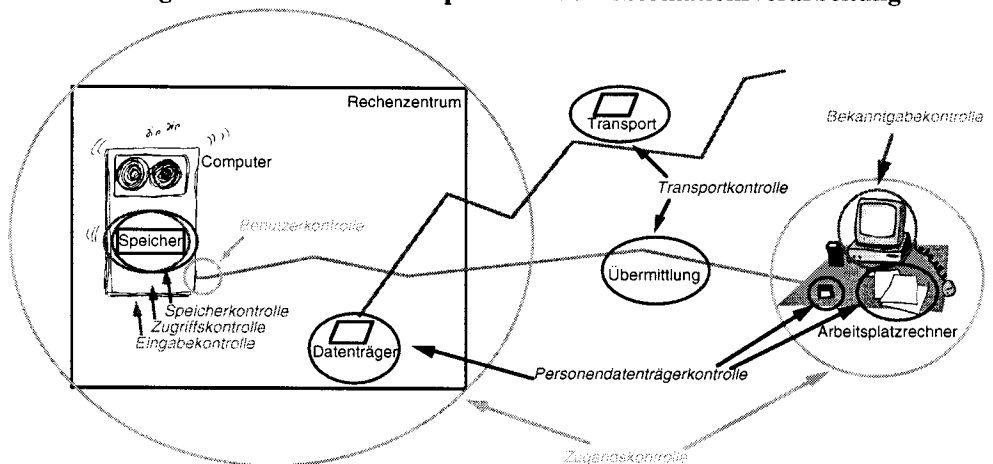
1 Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:

Name der Massnahme	Ziel der Massnahme			
	Vertraulichkeit	Verfügbarkeit	Richtigkeit	Nachvollziehbarkeit
a: Zugangskontrolle	X	(X)	(X)	
b: Personendatenträgerkontrolle	X	(X)	(X)	
c: Transportkontrolle	X	(X)	(X)	
d: Bekanntgabekontrolle				X
e: Speicherkontrolle	X	X	X	
f: Benutzerkontrolle	(X)	(X)	(X)	
g: Zugriffskontrolle	X	(X)	(X)	
h: Eingabekontrolle				X

- a *Zugangskontrolle*: unbefugten Personen ist der Zugang zu den Einrichtungen in denen Personendaten bearbeitet werden, zu verwehren;
- b *Personendatenträgerkontrolle*: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
- c *Transportkontrolle*: bei der Bekanntgabe von Personendaten, sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;
- d *Bekanntgabekontrolle*: Datenempfänger, denen Personendaten durch Einrichtungen zur Datenübertragung bekanntgegeben werden, müssen identifiziert werden können;
- e *Speicherkontrolle*: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;
- f *Benutzerkontrolle*: die Benutzung von automatisierten Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;
- g *Zugriffskontrolle*: der Zugriff der berechtigten Personen ist nur auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
- h *Eingabekontrolle*:

in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten, zu welcher Zeit und von welcher Person eingegeben wurden.

Zuordnung der Kontrollen zu Komponenten der Informationsverarbeitung



2 Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.