

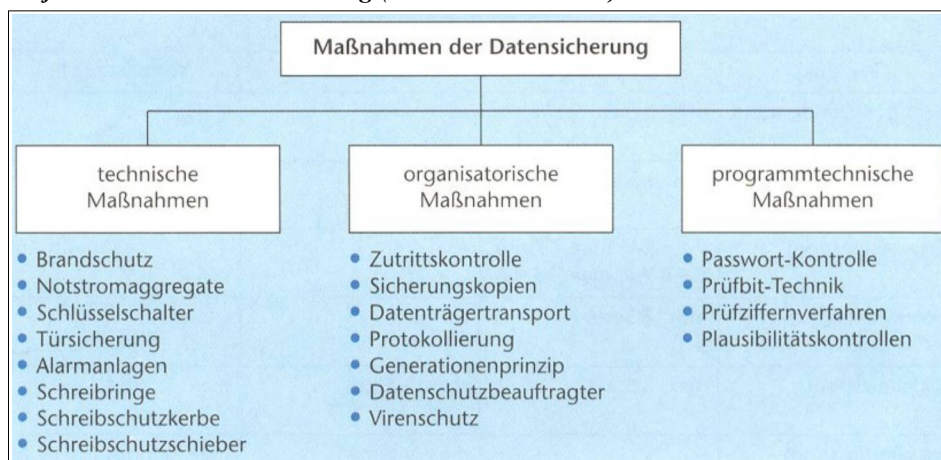


Problemsituation: In der IT-Welt werden die beiden IT-Fachbegriffe "**Datenschutz**" und "**Datensicherheit**" theoretisch peinlichst genau auseinander gehalten, d.h. insbesondere in der Wissenschaft und in den IT-Fach- und -Lehrbüchern! In der Praxis sieht dies oftmals leider etwas anders aus! Wir haben zu Beginn unseres BSN-Unterrichts zur Unterrichtreihe "IT-Security" über den kleinen aber feinen Unterschied dieser beiden Fachbegriffe gesprochen! Im NetIT-Lehrbuch erfolgt die Erklärung hierzu ebenfalls direkt zu Beginn des betreffenden Kapitels 14 (Netzwerksicherheit) in den beiden Unterkapiteln 14. 1 (Datenschutz) und 14. 2 (Datensicherheit). Definitionen dieser beider Fachbegriffe sollen hier kurz zusammengefasst werden:

- **Datenschutz:** Der "Datenschutz" dient dem Schutz des Bürgers bzw. dem Menschen vor missbräuchlicher Verwendung seiner Daten und ist gesetzlich geregelt (s. "Datenschutzgrundverordnung", kurz "DSVGVO"). Der Datenschutz dient ausdrücklich nicht dem Schutz der Daten (und der betreffenden IT-Geräte und IT-Systeme) selbst. Allgemein verständlich ausgedrückt ist der "Datenschutz" die Gewährleistung von Vertraulichkeit personenbezogener Daten vor Missbrauch, d.h. nur berechtigte Personen haben Zugang zu diesen personenbezogenen Daten.
- **Datensicherheit:** Die "Datensicherheit" dient dem Schutz der Daten selbst und der betreffenden IT-Geräte und IT-Systeme vor ihrem Verlust und ihrer Manipulation. Die vollständige Datensicherheit bedeutet die Gewährleistung von "Integrität" der Daten (Die Daten dürfen nicht von Unbefugten gelöscht oder manipuliert worden sein!) und die (zuverlässige) "Verfügbarkeit" der Daten (Die Daten müssen über das IT-System stets verfügbar sein und dürfen nicht, aufgrund eines Ausfalls von Hard- oder Software, blockiert werden).

Zur Gewährleistung einer möglichst hohen Datensicherheit existiert heute eine Vielzahl an Datensicherungsmaßnahmen, die entweder technischer, organisatorischer oder programmtechnischer Art sein können, wie das nachfolgende Bild aufzeigt.

Maßnahmen der Datensicherung (s. Gehlen-Lehrbuch)



Praxisbeispiele zur Umsetzung der Maßnahmen!


Es gibt keine vollständige (100%-ige) "Datensicherheit", da niemand garantieren kann, dass nicht doch ein Defekt der Hardware auftritt oder dass Daten von Personen mit unseriösen Absichten über unbekannte Kanäle manipuliert werden. Ziel ist es jedoch, eine möglichst hohe Datensicherheit zu erreichen, z.B. durch grundlegende Maßnahmen wie "Backup & Restore" (B&R), RAID, Server-Cluster, USV, IDS bzw. IPS, Firewalls, VPN etc.!

Die heutzutage existierenden mannigfachen technischen Möglichkeiten, Daten zu sammeln und auszuwerten, sorgen neben der Datensicherheit für eine stetig steigende Bedeutung des "Datenschutzes" und der Informationsfreiheit. Die Verpflichtung zur Einhaltung der Datenschutz-rechtlichen Vorschriften ist damit eine vorrangige Aufgabe in unserer heutigen Welt. Am 25.05.2018 ist die neue Datenschutz-Grundverordnung (DSGVO) der EU in Kraft getreten, wodurch wir alle endlich auch auf europäischer Ebene besser vor Datenmissbrauch geschützt werden sollen. Unser nationales und bereits seit 20.12.1990 gültiges "Bundesdatenschutzgesetz" (kurz "BDSG") ist dem DSGVO sehr ähnlich und zudem nur hierarchisch unterstellt.

Die grundlegenden Maßnahmen zur Datensicherheit (B&R, RAID, USV, VPN etc.) haben wir im Unterricht anhand des Übungsblattes "CI3Ox_Net-Sec-Basics-01.01_AUF.pdf" ausreichend behandelt. Hierzu möchte ich Ihnen noch bis Mitte der ersten Osterferienwoche ein zusammenfassendes, schriftliches Dokument als "LM-Musterlösung" über Moodle z.V. stellen, das Sie gleichzeitig auch zur gezielten Vorbereitung auf die anstehende BSN-Vorklausur (Termin laut IServ-Kalender-Eintrag am Montag, den 12.04.21) verwenden können! Bis dahin setzen Sie sich bitte zur weiteren gezielten Vorbereitung auf die BSN-Vorklausur etwas konkreter mit dem o.a. Thema "Datenschutz" auseinander. Machen Sie sich hierbei insbesondere mit den wichtigsten Maßnahmen des Datenschutzes vertraut, die im BDSG aufgeführt sind und als die „Zehn Gebote des Datenschutzes“ bezeichnet werden. Verwenden Sie hierzu das Kapitel 14 im NetIT-Lehrbuch und die nachfolgende Übungsaufgabe!

Die zehn Gebote des Datenschutzes (s. NetIT-Lehrbuch)

Maßnahme	Inhalt	Umsetzung
Zugangs-kontrolle	Nur Berechtigten ist der Zugang zur EDV- Anlage erlaubt.	Die Anlage wird durch ein Zugangskontrollsystem („Closed Shop“-Betrieb) geschützt.
Daten-träger-kontrolle	Der Datenträger muss gegen Diebstahl geschützt werden.	<ul style="list-style-type: none"> • Datenträger müssen an einem sicheren Ort aufbewahrt werden. • Nur Berechtigte haben Zugang zum Datenträger.
Speicher-kontrolle	Eine Manipulation des Speicherinhaltes muss verhindert werden.	<ul style="list-style-type: none"> • Es gibt einen Schutz durch eingeschränkte Zugriffsberechtigungen. • Nur Berechtigte dürfen auf die Daten zugreifen. • Es findet eine Kontrolle durch Datenvergleich statt.
Benutzer-kontrolle	Nur Berechtigte dürfen die EDV benutzen.	Es wird ein Schutz durch eine Benutzeridentifizierung vorgenommen ¹ .
Zugriffs-kontrolle	Nur Berechtigte dürfen auf Informationen zugreifen.	Dateiberechtigungen und Benutzerrechte werden eingerichtet.
Übermitt-lungs-kontrolle	Wer, wann, wohin, welche Daten übermittelt hat wird kontrolliert.	Alle Transaktionen werden protokolliert.
Eingabe-kontrolle	Wer welche Daten eingibt wird kontrolliert.	Wer welche Daten zu welchem Zeitpunkt eingegeben hat wird protokolliert.
Auftrags-kontrolle	Es wird kontrolliert, dass nur auftragsgemäß Daten verarbeitet werden.	Wer welchen Auftrag erteilt wird protokolliert.
Transport-kontrolle	Es muss sichergestellt werden, dass bei der Übermittlung von Daten und dem Transport von Datenträgern keine Manipulation und Einsicht in die Daten möglich ist.	<ul style="list-style-type: none"> • Nur Berechtigte transportieren Datenträger und übermitteln Daten. • Die Personen werden auf das Datengeheimnis verpflichtet.
Organisations-kontrolle	Die gesamte betriebliche Organisation muss datenschutzgerecht sein.	Umsetzung der Datenschutzrichtlinien.

CI3Ox	BSN – "Netzwerksicherheit" – Übung	20.12.21	 Berufskolleg Ostvest
"Datenschutz vs. Datensicherheit"			

Übung zum Thema "Datenschutz":

Ausgangssituation: Sie buchen eine Reise bei einem Reiseunternehmen. Die Mitarbeiterin im Reisebüro gibt hierzu Ihre Anschrift in den Computer ein. Die Adresse wird in einer Datei auf dem Computer gespeichert. Mit der Speicherung der Daten hat der DV-Anwender besondere Pflichten. Der "Datenschutz" stellt personenbezogene Daten unter einen besonderen Schutz.

Hierbei hat 2018 die Datenschutzgrundverordnung (DSGVO) das alte, bereits seit 1990 geltende Datenschutzgesetz (BDSG) abgelöst. Nachfolgend ein paar Auszüge zu den Pflichten von DV-Anwendern im Umgang mit Personen-bezogenen Daten, jeweils aus der "alten" BDSG und aus der "neuen" DSGVO zum direkten Vergleich miteinander:

Pflichten von DV-Anwendern nach der alten BDSG:

§1 Datenschutzgesetz – Zweck und Anwendungsbereich des Gesetzes

Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

§6 Datenschutzgesetz – Technische und organisatorische Maßnahmen:

Werden personenbezogene Daten automatisch verarbeitet, sind zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind.

Pflichten von DV-Anwendern nach der neuen DSGVO:

Artikel 2 – Sachlicher Anwendungsbereich:

- (1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Artikel 24 - Verantwortung des für die Verarbeitung Verantwortlichen:

- (1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
- (2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

Hieraus ergeben sich bestimmte Pflichten für alle, die Personen-bezogene Daten erheben, verarbeiten oder nutzen. Maßnahmen müssen geeignet sein, die Daten zu schützen, denn so steht es im Datenschutzgesetz. Hieraus leiten sich für den DV-Anwender die folgenden zehn "Pflichten" (Gebote) des Datenschutzes ab, d.h. die

1. *Abgangskontrolle,*
2. *Auftragskontrolle,*
3. *Benutzerkontrolle,*
4. *Eingabekontrolle,*
5. *Organisationskontrolle,*
6. *Speicherkontrolle,*
7. *Transportkontrolle,*
8. *Übermittlungskontrolle,*
9. *Zugangskontrolle,*
10. *Zugriffskontrolle.*

Aufgabe 1: Ordnen Sie die oben angegebenen Begriffe für "Pflichten" des verantwortlichen DV-Anwenders den nachfolgenden Beschreibungen entsprechend zu!

Beschreibung	Begriff
(1) Unberechtigten ist der Zugang zur DV-Anlage mit der personenbezogene Daten verarbeitet werden, zu verwehren.	
(2) Personen, die in der DV tätig sind, sind daran zu hindern, dass sie Datenträger entfernen.	
(3) Die unbefugte Eingabe sowie Kenntnisnahme, Veränderung oder Löschung ist zu verhindern.	
(4) Die Nutzung des Datenverarbeitungssystems durch Unbefugte ist zu verhindern.	
(5) Der Zugriff der Zugangsberechtigten ist nur auf die für ihn relevanten Daten einzugrenzen.	
(6) Es muss überprüfbar sein, an wen und wie personenbezogene Daten übermittelt werden.	
(7) Es muss überprüft und festgestellt werden können, von wem und wann personenbezogene Daten eingegeben worden sind.	
(8) Die personenbezogenen Daten dürfen nur so verarbeitet werden, wie es vom Auftraggeber vorgegeben wurde.	
(9) Bei der Übermittlung und beim Transport müssen Daten bzw. Datenträger vor unbefugtem Lesen, Verändern und Löschen gesichert sein.	
(10) Die Organisation einer Behörde oder eines Betriebes muss geeignet sein, dass alle Datenschutzbestimmungen erfüllt werden können.	

Aufgabe 2: Überlegen und beschreiben Sie schriftlich für jede o.a. Pflicht, durch welche Maßnahmen das Reisebüro die beschriebenen Pflichten zum Schutz der personenbezogenen Daten einhalten kann. Geben Sie hierbei passende Beispiele für technische Umsetzungen an.

Aufgabe 3: Oft fällt das Fachwort Vertraulichkeit in der IT-Welt.

[3.1] Was bedeutet Vertraulichkeit von Daten (1 Satz)?

[3.2] Welche SW-technische Maßnahme realisiert die Vertraulichkeit von Daten in der IT-Welt (1 Option)?

[] Datensicherung. [] RAID. [] Verschlüsselung. [] VLAN. [] USV. [] Firewall.

Musterlösung:

Ausgangssituation: Sie buchen eine Reise bei einem Reiseunternehmen. Die Mitarbeiterin im Reisebüro gibt hierzu Ihre Anschrift in den Computer ein. Die Adresse wird in einer Datei auf dem Computer gespeichert. Mit der Speicherung der Daten hat der DV-Anwender besondere Pflichten. Der "Datenschutz" stellt personenbezogene Daten unter einen besonderen Schutz.

Hierbei hat 2018 die Datenschutzgrundverordnung (DSGVO) das alte, bereits seit 1990 geltende Datenschutzgesetz (BDSG) abgelöst. Nachfolgend ein paar Auszüge zu den Pflichten von DV-Anwendern im Umgang mit Personen-bezogenen Daten, jeweils aus der "alten" BDSG und aus der "neuen" DSGVO zum direkten Vergleich miteinander:

Es folgen Auszüge aus dem BDSG und der DSGVO ... (s.o.)!

Aufgabe 1: Ordnen Sie die oben angegebenen Begriffe für "Pflichten" des verantwortlichen DV-Anwenders den nachfolgenden Beschreibungen entsprechend zu!

Beschreibung	Begriff
(1) Unberechtigten ist der Zugang zur DV-Anlage mit der personenbezogene Daten verarbeitet werden, zu verwehren.	Zugangskontrolle
(2) Personen, die in der DV tätig sind, sind daran zu hindern, dass sie Datenträger entfernen.	Abgangskontrolle (Datenträgerkontrolle)
(3) Die unbefugte Eingabe sowie Kenntnisnahme, Veränderung oder Löschung ist zu verhindern.	Speicherkontrolle
(4) Die Nutzung des Datenverarbeitungssystems durch Unbefugte ist zu verhindern.	Benutzerkontrolle
(5) Der Zugriff der Zugangsberechtigten ist nur auf die für ihn relevanten Daten einzugrenzen.	Zugriffskontrolle
(6) Es muss überprüfbar sein, an wen und wie personenbezogene Daten übermittelt werden.	Übermittlungskontrolle
(7) Es muss überprüft und festgestellt werden können, von wem und wann personenbezogene Daten eingegeben worden sind.	Eingabekontrolle
(8) Die personenbezogenen Daten dürfen nur so verarbeitet werden, wie es vom Auftraggeber vorgegeben wurde.	Auftragskontrolle
(9) Bei der Übermittlung und beim Transport müssen Daten bzw. Datenträger vor unbefugtem Lesen, Verändern und Löschen gesichert sein.	Transportkontrolle
(10) Die Organisation einer Behörde oder eines Betriebes muss geeignet sein, dass alle Datenschutzbestimmungen erfüllt werden können.	Organisationskontrolle

Aufgabe 2: Überlegen und beschreiben Sie schriftlich für jede o.a. Pflicht, durch welche Maßnahmen das Reisebüro die beschriebenen Pflichten zum Schutz der personenbezogenen Daten einhalten kann. Geben Sie hierbei passende Beispiele für technische Umsetzungen an.

Lösungsansatz: s.o., Tabelle "Die zehn Gebote des Datenschutzes (s. NetIT-Lehrbuch)", 3. Spalte unter "Umsetzung"! Für jede Situation lassen sich leicht für jede dieser 10 Pflichten/Regeln ein passendes Praxisbeispiel mit entsprechender technischer, organisatorischer oder Programm-technischer Umsetzung (s.o., "Maßnahmen der Datensicherung") finden und beschreiben! In der konkreten Situation dieser Aufgabe, d.h. für das Reisebüro sind beispielsweise vom Reisebüro-Inhaber und den hier zuständigen Angestellten folgende Pflichten bzw. Regeln im Umgang mit den verschiedenen Personen- bzw. Kundendaten zu beachten und praktisch umzusetzen:

- **Zugangskontrolle:** Die eingegebenen Personendaten auf dem lokalen Reisebüro-Computer müssen so technisch geschützt sein, dass kein Unbefugter an diese Daten gelangen kann, s. z.B. per User-Login (User Account: Username & Password), weiter z.B. auf Datei-Ebene durch Verschlüsselung der Datei bzw. durch Datei-Schreibschutz (Zugang an verschlüsselte Datei per Passwort) etc.! Es ist stets darauf zu achten, dass der Computer (z.B. per Abmeldung, Herunterfahren und Ausschalten des PC ...) verschlossen ist und so

keiner an die Daten gelangen kann. Ein zentralisiertes Server-Netzwerk würde die Sicherheit im Reisebüro enorm erhöhen (s.u.)!

- **Abgangskontrolle (Datenträgerkontrolle):** Das Speichermedium (HDD, SSD) des lokalen Computers und damit auch der Computer selbst muss jederzeit (insbesondere auch bei Ladenschluss!) so sicher aufbewahrt bzw. abgestellt/untergebracht und kontrolliert sein, dass kein Unbefugter Medien/Computer entwenden können und damit "Datenklau" betreiben können. I.d.R. ist in dieser Situation minimal eine Alarmanlage zur Kontrolle vorhanden. Ansonsten sollte der Computer an einem sicheren Ort stehen, an dem nicht jeder Unbefugte leicht gelangen kann! Hier wäre ein Server-, noch besser Terminal-Netzwerkssystem angebrachter mit viel mehr Sicherheit! Am Terminal oder auch per Thinclient wird exklusiv die Ein- und Ausgabe der Daten vorgenommen, während die Daten per Netz auf dem Server zentral gespeichert werden. Terminal bzw. Thinclient muss nicht 24 h pro Tag sicher aufbewahrt bzw. überwacht sein, wobei der Server aber schon an einem sicheren Ort (z.B. abgeschlossener Raum) steht!
- **Benutzerkontrolle:** Jeder Berechtigte sollte wie bereits neben der Zugangskontrolle (s.o.) erwähnt ein spezielles User Account haben, womit auch die Pflicht der Benutzerkontrolle erfüllt wird: Nur befugte Benutzer können individuelle entsprechend ihrer Berechtigung Daten erstellen, einsehen, ändern und löschen!
- **3er-Kombination von Übermittlungs-, Auftrags- und Eingabekontrolle:** Alle Transaktionen am Computer ist entsprechend (systematisch wie manuell) zu protokollieren, auf OS-Eben (z.B. per Logfiles) und auf Anwendungsebene (per vertikaler bzw. Reisebüro-spezifischer DV- & Transaktions-App), damit überprüfbar ist, wann und wofür welche Kundendaten bearbeitet hat.
- **Transportkontrolle:** Wenn der Computer beispielsweise lokal gesichert wird (s. "Backup & Restore"), z.B. per Vollsicherung auf einem Speichermedium wie USB-Stick, Streamer, Band etc., sind die Medien mobil! Die Mobilität per "Transport", Weglegen, deponieren muss per befugte Vertrauensperson an einem sicheren Ort zur Aufbewahrung erfolgen! Die Daten auf einem mobilen Datenträger (DVD, USB-Stick, Magnetband etc.) sind vor unbefugtem Lesen, Verändern und Löschen zu sichern. Alle befugten Personen, die Daten einsehen bzw. lesen können, sind dem Datengeheimnis verpflichtet!
- **etc. ... !!!**

Aufgabe 3: Oft fällt das Fachwort Vertraulichkeit in der IT-Welt.

[3.1] Was bedeutet Vertraulichkeit von Daten (1 Satz)?

→ **Keine Weitergabe der Daten an Unbefugte erlauben bzw. keinen Zugriff auf die Daten durch Unbefugte erlauben!**

[3.2] Welche SW-technische Maßnahme realisiert die Vertraulichkeit von Daten in der IT-Welt (1 Option)?

[] Datensicherung. [] RAID. ☒ Verschlüsselung. [] VLAN. [] USV. [] Firewall.