Modul 231 Zusammenfassung

Ein Bild, das Text, Kreis, Screenshot, Compact Disc enthält.

Automatisch generierte Beschreibung**Der Begriff Privat:** Es existiert keine allgemeingültige Definition des „Privaten“. Bei der Privatsphäre handelt es sich vielmehr um eine Idee, die historisch, kulturell und situationsspezifisch Veränderungen unterworfen ist. „Privat“ leitet sich vom lat. Begriff „privatus“ ab, der in der Übersetzung „(Der Herrschaft) beraubt, gesondert, für sich stehend“ bedeutet und damit die Trennung von der öffentlichen Sphäre meint – vor allem vom Staat. Im alltäglichen Gebrauch ist „privat“ oft die Opposition zu „öffentlich“. Privatsphäre von Personen kann nicht nur Räumen oder Orten zugeschrieben werden. Handlungen, Situationen, mentale Zustände und Gegenstände können privat sein. Öffentlich und privat kann man sich räumlich gut mit den Schichten einer Zwiebel vorstellen:

Warum ist Privatsphäre wichtig? Die Privatsphäre bietet einen geschützten Raum, in dem wir unabhängig von Beeinflussungen anderer agieren können und damit authentisch und selbstbestimmt die sein können, die wir sein wollen. Hier können wir ohne Zwänge frei nachdenken, uns ausprobieren und unsere Meinung bilden. Die Privatsphäre hat zudem vier zentrale Funktionen:

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

**Daten:** Daten sind durch Beobachtungen, Messungen, statistische Erhebungen beruhende Angaben oder formulierbare Befunde. Man unterscheidet dann noch zwischen den Daten und den „personenbezogenen Daten“. Personenbezogene Daten sind Daten, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann. Sie erlauben Rückschlüsse über diese Person. Diese Daten verdienen besonderen Schutz.

**Kategorisierung von Daten**

Wer personenbezogene Daten verarbeitet, der sollte wissen, was für Kategorien das Gesetz vorsieht. Je nach Kategorie sind verschiedene Verarbeitungsmethoden zugelassen, ausserdem gelten verschiedene Vorschriften, wie diese Daten vernichtet werden müssen. Im Gesetz ist definiert, was personenbezogene Daten sind. Es ist die Rede von „Personendaten“. Personendaten sind Daten, die die Identifikation eines Menschen direkt oder indirekt ermöglichen. Warum werden diese Daten kategorisiert? Der Gesetzgeber sieht vor, dass personenbezogene Daten einer unterschiedlichen Schutzbedürftigkeit unterliegen. Das heisst, dass manche Informationen strenger geschützt werden müssen als andere.

**Das Datenschutzrecht unterscheidet zwischen Personendaten und besonders schützenswerte Personendaten.**

**Kundenprofiling**

Kundenprofiling bedeutet, dass man die Kunden in verschiedene Gruppen kategorisiert um so gezielt besser auf die Präferenzen des Kunden eingehen zu können. Ziel des Unternehmens ist hierbei die Umsatzsteigerung oder auch die Neukundengewinnung. Aus gewissen Produkten kann man beispielsweise ableiten, dass eine Person schwanger oder aktuell krank ist. Zudem lässt sich sehr oft and den Produkten oder den getätigten Einkäufen das Geschlecht oder ein ungefähres Alter ermitteln.

Wie kann man sich vor Kundenprofiling schützen? Man kann beispielsweise bewusst auf Karten wie etwa die „Cummulus Karte“ verzichten, zudem hilft es, auch wenn man mit Bargeld bezahlt. Anti Tracking Add-Ons verwenden.

**Das Privacy-Paradox**

Obwohl Menschen schon seit einigen Jahren sensibilisiert werden, dass man im vor allem im Internet auf seine persönlichen Daten aufpassen muss, gibt es nach wie vor das Privacy Paradox. Damit wird das Phänomen beschrieben, dass die Nutzer den Schutz ihrer Privatsphäre zwar generell für wichtig halten, dies aber nicht unbedingt auf ihr Handeln übertragen. Beispielsweise wissen viele dass WhatsApp nicht die ideale App ist wenn es um Datenschutz geht, jedoch benutzen weiterhin die meisten Menschen weiterhin noch WhatsApp, da der Aufwand bis alle wieder auf eine weitere App umgestiegen sind zu gross wäre und die Menschen gerne das beibehalten, an was sie sich gewöhnt sind.

**Veränderung der Privatsphäre seit Einführung des Social Web**

Daten sind für jeden viel greifbarer geworden. Nachteil ist, dass jeder viel einfacher Zugriff auf meine Daten hat. Beispielsweise könnte ein Arbeitgeber ein peinliches Video von mir sehen, dies könnte negative Folgen haben. Jeder kann Informationen veröffentlichen, zudem ist es nicht mehr so einfach Daten wieder aus dem Internet zu löschen, wenn diese erstmals in Umlauf sind. Zudem fehlt auch vielen Menschen die Sensibilität. Daraus ergeben sich auch viele Nachteile. Kriminellen fällt es so oft leichter Identitätsdiebstahl zu begehen, im schlimmsten Fall kann man auch gestalkt werden. Phishing und Betrug, soziale und berufliche Auswirkungen wie etwa Rufschädigung sind mögliche negative Folgen der Zugänglichkeit unserer Daten im Netz.

**Datenschutzgesetz:**

[SR 235.1 - Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG) (admin.ch)](https://www.fedlex.admin.ch/eli/cc/2022/491/de)

Im Datenschutzgesetz ist alles geregelt was die mit Daten und wie sie geschützt oder auch beispielsweise vernichtet werden müssen geregelt. Diese Daten sind unter anderem auch personenbezogene Daten. Unternehmen sind verpflichtet mitzuteilen, was für Daten sie alles über eine Person sammeln, jedoch akzeptiert man dies meistens, wenn man die AGBs unterschreibt. Oft ist es jedoch erschreckend, wenn man erfährt, was Unternehmen alles über einen wissen. Ein Beispiel wäre hier Google.

**Datensicherheit:** Datensicherheit ist ein mit dem Datenschutz eng verknüpfter Begriff, welcher jedoch von dem zu differenzieren ist. Datensicherheit betrifft alle Daten, egal ob Personendaten oder nicht. Auch ist es egal ob diese Daten in digitaler oder analoger Form vorhanden sind. Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Masse gegen Manipulation, Verlust, unberechtigte Kenntnisnahme durch Dritte oder andere Bedrohungen zu sichern. Datensicherheit ist ein angestrebter Zustand, welcher unter anderem Datenschutzmassnahmen erreicht werden soll. Zudem gibt es noch Datenschutz und Datensicherheitskonzepte. In einem Datenschutzkonzept werden die für eine datenschutzrechtliche Beurteilung notwendigen Informationen zur Erhebung, Nutzung und Verarbeitung personenbezogener Daten beschrieben. Ein Datensicherheitskonzept dient primär dem Ziel der Informationssicherheit und **berücksichtigt im Gegensatz zum Datenschutzkonzept alle Daten, egal ob analog oder digital, egal ob personenbezogen oder nicht.**

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Datensicherheit im Datenschutzgesetz

Wichtige Punkte im DSG zum Thema Datenschutz:

Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Bei Artikel 7 im DSG sind ebenfalls Infos zu Datensicherheit.

**Problembereiche im Thema Datensicherheit**

Die Datensicherheit umfasst folgende Problembereiche.

Höhere Gewalt (Sturm, Erdbeben)

Menschliche Handlungen (löschen von Daten, Datendiebstahl,)

Technische Störungen (Stromausfall, Hardwaredefekt)

Bei höherer Gewalt eignet es sich beispielsweise mehrere Standorte zu haben (Redundanz) oder beispielsweise ein Cloud Backup. Bei menschlichen Handlungen eignen sich ebenfalls Back Ups, Kryptographie, Zugriffskonzepte (Authentifizierung/Autorisierung), Speichermedien sperren oder eine Firewall/Virenscanner. Bei technischen Störungen sind Back Ups und redundante Komponente geeignet.

Ein Bild, das Text, Screenshot, Schrift enthält.

Automatisch generierte BeschreibungBerühmte Vorkommnisse

Bei Unternehmen beispielsweise können solche Vorkomnisse sehr rufschädigend sein und auch sehr kostspielig werden. Oft müssen sich Unternehmen noch bessere Massnahmen überlegen, um die Daten gerecht zu sichern oder sie beispielsweise verschlüsseln. Bei dem NSA-Skandal kann auch beispielsweise der Ruf mehrerer Länder und das Vertrauen in die Regierung verloren gehen. Menschen, welche herausgefunden haben was mit den Daten wirklich gemacht wird oder gewisse Daten an die Öffentlichkeit bringen, riskieren oft rechtliche Konsequenzen.