Wissensnugget Datenmanagement

Inhalt

Legende:

Blau hinterlegte Texte sind auf Basis-Level, d.h. beinhalten Grundlagenwissen für Studierende aller Fachbereiche,

Grau hinterlegte Texte sind auf Expert Level, d.h. für Studierende aus den Studiengängen (Wirtschafts-)informatik und Management und Recht.

Ohne Hintergrundfarben sind Übergänge zwischen Abschnitte, weiterführende Erläuterungen und nice to have Informationen.

1 Datenmanagement für einen sinnvollen Umgang mit Daten

In modernen Unternehmen fallen tagtäglich Unmengen von Datensätzen an. Dank **elektronischer Datenverarbeitung (EDV)** ist das Erfassen und Organisieren der Informationen eigentlich kein Problem mehr. Kundendaten können in Datenbanken erfasst werden, die Mitarbeiterverwaltung lässt sich automatisieren. Dazu muss der Rechner nur mit ausreichend Daten gefüttert werden, ausgeklügelte Algorithmen übernehmen den Rest.

Doch mit der zunehmenden Vernetzung und der **steigenden Datenflut** entstehen neue Probleme. Mehrere Mitarbeiter müssen auf denselben Datenbestand zugreifen, und zwar möglichst gleichzeitig. Daten sollen nicht mehrfach erfasst werden und jederzeit auffindbar sein. Doch vor allem müssen sie sicher sein vor Verlust durch Hardware-Defekte oder fehlerhafte Bedienung und abgeschirmt vor Hackern und sonstigen Datendieben im Internet.

Dabei sind nicht zuletzt rechtliche Aspekte zu beachten, d. h. Aufbewahrungsfristen, Einverständniserklärungen zur Speicherung personenbezogener Daten, um nur Teilbereiche des

Datenschutzes zu nennen. Die Komplexität dieses Themenbereichs hat zur Entwicklung einer **neuen Disziplin** in der Informationstechnik geführt, dem Datenmanagement

1.1 Datenmanagement – Definition und Begriffserklärung

Datenmanagement (oder Data Management) stellt bestimmte Anforderungen an den Umgang mit digitalen Daten. Der Begriff beschreibt eher einen Prozess als einzelne Massnahmen. Bereits beim Erheben und Eingeben von Daten müssen diese organisiert werden. Datensparsamkeit und -qualität sind zwei Faktoren, die hier zu berücksichtigen sind. Neben dem Schutz der Inhalte sollen die Daten nicht zuletzt effektiv für den eigentlichen Erfassungszweck verwendbar sein, d. h. die Praxistauglichkeit darf bei allen Bemühungen nicht zu kurz kommen. Schliesslich sollte man sich im Rahmen des Datenmanagements auch fragen, welche Daten für welchen Zeitraum archiviert werden müssen. Nicht benötigte Daten muss man schnell auffinden und sicher löschen können.
Das Datenmanagement muss möglichst praktikabel und intuitiv in die Abläufe eingebunden werden. Dies sorgt für die beste Akzeptanz bei den Mitarbeitenden und die grösstmögliche Effektivität. Einige der vorgestellten Ziele sind auch im Hinblick auf die **Effizienzsteigerung** sinnvoll. Das Erheben unnötiger Daten kostet Zeit und verärgert womöglich die Kunden oder Anwender. Die geordnete und sichere Ablage von Daten verbessert die Produktivität.
Es kann daher sinnvoll sein, eine **Data-Governance-Richtlinie** einzuführen, in der festgelegt wird, wie mit den Daten umzugehen ist. Dies betrifft insbesondere die Datenqualität und mögliche Verbesserungen durch Hilfen wie Autokorrekturen. Ausserdem werden einheitliche Formulierungen und Begriffe definiert.

1.1.1 Definition: Datenmanagement

Basic-Level

Der Begriff Datenmanagement beschreibt ein ganzheitliches Konzept zum Umgang mit digitalen Daten. Das Datenmanagement umfasst alle Schritte vom Erheben, über das Speichern und die Verarbeitung bis hin zur Archivierung und Löschung. Dabei sollen Erfordernisse des Unternehmens genauso berücksichtigt werden wie Aspekte der Datensicherheit und des Datenschutzes.

1.1.2 Arten von Daten

Um den Umgang mit Daten zu planen, sollten Sie sich zunächst die Frage stellen, welche Arten von Daten bei Ihnen anfallen. Hier kann das Einteilen in **Kategorien** helfen, um systematisch vorzugehen und keinen Bereich zu übersehen:

1.1.2.1 Personenbezogene Daten bzw. Personendaten

Personenbezogene Daten sind Informationen, die sich unmittelbar auf bestimmte Personen beziehen; klassische Beispiele sind Namen, Rufnummern und Adressen. Doch auch Messdaten und das Einkaufsverhalten zählen dazu. Es kann sich um Kundendaten, Daten eigener Mitarbeiter oder von Drittpersonen handeln. Diese Daten geniessen allgemein rechtlichen Schutz.
Die EU-Datenschutz-Grundverordnung definiert „**personenbezogene Daten**“ wie folgt: Personenbezogen sind alle Daten, die folgendes enthalten:

- Informationen, die eine direkte Identifizierung möglich machen – zum Beispiel Namen, Vornamen, Telefonnummern usw.
- Pseudonymisierte Daten oder Informationen, die keine direkte Identifizierung von Nutzern erlauben, die es aber möglich machen, das Verhalten von einzelnen Nutzern zu erfassen (um ihr oder ihm zum Beispiel im richtigen Moment die richtige Werbung anzuzeigen)

Die EU-Datenschutz-Grundverordnung unterscheidet klar zwischen Informationen, die eine direkte Identifizierung ermöglichen, und pseudonymisierten Daten. Die EU-Datenschutz-Grundverordnung fördert die Nutzung pseudonymisierter Informationen; sie besagt ausdrücklich: „Der Einsatz von Pseudonymisierung bei der Verarbeitung von personenbezogenen Daten minimiert die Risiken für die Betroffenen und unterstützt die Datenverantwortlichen dabei, ihre Verpflichtungen in Sachen Datenschutz zu erfüllen.“

Das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020 (auch (nDSG oder revDSG bezeichnet) definiert **Personendaten** wie folgt:

- alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

1.1.2.2 Sensible oder besonders schützenswerte Personendaten

In der Eu gelten die folgenden personenbezogenen Daten als „sensibel“ und unterliegen **besonderen Verarbeitungsbedingungen**:

- personenbezogene Daten, aus denen rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen einer Person hervorgehen;
- Gewerkschaftszugehörigkeit;
- genetische Daten, biometrische Daten, die ausschließlich zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden;
- Gesundheitsdaten;
- Daten zum Sexualleben oder zur sexuellen Orientierung einer Person.

Entsprechend definiert das nDSG **besonders schützenswerte Personendaten**:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
- Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
- genetische Daten,
- biometrische Daten, die eine natürliche Person eindeutig identifizieren,
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
- Daten über Massnahmen der sozialen Hilfe;

Wenn das Bekanntwerden solcher Daten zur Bedrohung, insbesondere an Leib und Leben der betroffenen Person führen kann, dann spricht man auch von **hochsensiblen (lebenswichtigen) Personendaten**.

1.1.2.3 Schützenswerte Firmendaten

Firmeninterna wie Buchhaltungsdaten, Steuerunterlagen und Firmengeheimnisse; hier wird jede Firma ohnehin ein besonderes Interesse am sorgsamen Umgang mit den Daten haben. Es ist aber durchaus sinnvoll, im Rahmen des Datenmanagements festzulegen, welche Informationen zu diesem Bereich gehören.

1.1.2.4 Sekundärdaten

Daten, die im Rahmen einer Massnahme für einen anderen Zweck entstehen; ein Beispiel wäre die Videoüberwachung, die üblicherweise zum Schutz vor Einbruch und Diebstahl installiert wird. Diese zeichnet möglicherweise auch Kennzeichen von Kundenfahrzeugen auf. Ein anderes Beispiel sind Logprotokolle im Firmennetzwerk, die möglicherweise IP-Adressen von Besuchern speichern.

*1.1.2.5 Öffentliche **Daten***

Absichtlich veröffentlichte und verbreitete Daten; dazu zählen Informationen auf der Internetpräsenz und in Firmenbroschüren. Wichtig ist hierbei die Einhaltung von Urheberrechtsvorschriften und der Schutz eigener Daten, etwa veröffentlichter Bilder, Werbeslogans und Firmenlogos. Letztere können nach dem Designgesetz (ehemals Geschmacksmustergesetz) geschützt werden.

1.1.3 Profiling

Der Begriff “Profiling” erhält im neuen Schweizer Datenschutzgesetz eine grosse Relevanz.
Als Profiling werden Kundendaten beschrieben, mithilfe derer sich ein genaues Bild über einen Menschen machen lässt. Dazu zählen Merkmale wie der Wohnort einer Person, ihre Hobbys und Interessen. Aber auch Daten wie die Entwicklung der

Arbeitsleistung, wirtschaftliche Verhältnisse oder Angaben über den Gesundheitszustand eines Menschen gehören dazu.
Mit hoher Sensibilität verarbeitet werden dürfen solche Daten künftig zwar weiterhin, aber nur, sofern sie die Persönlichkeitsrechte nicht ausdrücklich verletzen. Wenn eindeutig Wesenszüge einer Person abzulesen sind, handelt es sich um "Profiling mit hohem Risiko". Hierbei muss vorab immer eine ausdrückliche Einwilligung der Person erfolgen.

Basic-Level

1.1.4 Risikostufen

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 Zeu-ginnen und Zeugen in bestimmten Strafverfahren oder von Personen, die aufgrund ihrer Gesinnung oder ihrer religiösen oder politischen Zugehörigkeit bedroht sind.

1.2 Datenmanagement – Aufgaben und Umsetzung

Datenmanagement hat die Aufgabe, alle Prozesse vom Erheben bis zur Ablage oder Löschung von Daten zu integrieren und dabei die Effizienz zu berücksichtigen. Es wird die gesamte „Lebensdauer" betrachtet. Hieraus leitet sich der Begriff des **Data Life Managements (DLM)** ab.

1.2.1 Datenerhebung

Die Datenverarbeitung beginnt mit der Datenerhebung. Wichtig ist hierbei die Datensparsamkeit: Es sollten nur die nötigsten Informationen gesammelt werden. Diese Pflicht wurde inzwischen auch in der Europäischen Datenschutzgrundverordnung (DSGV)O) und im neuen **Schweizerischen Datenschutzgesetz** (auch nDSG oder revDSG bezeichnet) festgeschrieben. Personenbezogene Daten dürfen demnach nur dann verarbeitet werden, wenn Betroffene ihre Einwilligung gegeben haben oder dies aus rechtlichen Gründen notwendig ist, etwa bei einer Vertragsgestaltung.
Die Datenqualität lässt sich am effektivsten bei der Eingabe gewährleisten. Das sorgfältige Erfassen erspart unnötige Nachfragen und Nachbearbeitungen. Die Informationen sollten auch gleich in dem Format gespeichert werden, in dem sie später benötigt werden. Jede Übertragung oder Konvertierung kann zu Fehlern im Datenbestand führen.

Basic-Level

1.2.2 Datenspeicherung

Wichtig ist die Auswahl des **Speicherorts** und des -**formats**. Als Speicherort ist neben der lokalen Ablage eine Sicherung im Cloudspeicher denkbar. Beide Lösungen haben Vor- und Nachteile. Lokale Speicher lassen sich leichter vor fremdem Zugriff abschirmen. Cloud-Speicher hingegen sind besser skalierbar und ausfallsicher. Für sehr wichtige Daten bieten sich kombinierte Lösungen an.
Bei grossen Datenmengen sind Datenbanken erste Wahl für die Ablage. Wird **spezielle Software** verwendet, etwa für die Buchhaltung oder die Lagerhaltung, stellt sich die Frage nach dem

Speicherort ohnehin nicht. Bei letzterer sollte allerdings auf die Kompatibilität zu externen Systemen und Exportmöglichkeiten geachtet werden.

1.2.3 Datensicherheit (vgl. auch Wissensnugget 1.3)

Datensicherheit ist ein wichtiges und komplexes Thema beim Datenmanagement. Die Daten sollen vor **Verlust, ungewollter Veränderung und unberechtigten Zugriffen** geschützt werden. Hilfreiche und sehr ausführliche Informationen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI). In seinem laufend aktualisierten IT-Grundschutz-Kompendium werden mögliche Gefahren systematisch aufgezeigt. Neben den Risiken werden Prozessbausteine zur Absicherung aufgezeigt. Das Kompendium ist kostenlos verfügbar. Ein weiterer Vorteil ist, dass Zertifizierungen gemäss ISO 27001 (wie die Zertifizierung zur Informationssicherheit) darauf aufbauen.
Mögliche Gefahren sind:

- Hardware-Schäden durch Brand, Wasser oder Überspannung
- Datenverlust durch Fehlbedienung
- Datenverlust oder Funktionsuntüchtigkeit der Systeme durch Schadsoftware (Verschlüsselungstrojaner, Datendiebstahl)
- Datenverlust durch Software-Fehler
- Verlust durch Diebstahl

Um den verschiedenen Risiken zu begegnen, umfassen Lösungen nicht nur softwaregestützte Schutzmechanismen, sondern auch organisatorische Massnahmen wie Brand- und Einbruchmeldeanlagen.

Basic-Level

Diese Grundsätze sollten Sie beachten:

- Regelmässige Updates: Dabei gilt es zwischen automatisierten und manuellen Updates abzuwägen. Vorteil automatisierter Updates ist, dass man sie nicht vergisst. Für das manuelle Einspielen spricht, dass man fehlerhafte Updates vermeidet.
- Sichere Passwörter: Auch hier gibt es unterschiedliche Strategien. Sinnvoll ist es, die Mitarbeiter durch Vorgaben zu zwingen, komplexe Passwörter zu verwenden. Auch das regelmässige Ändern von Kennwörtern ist sinnvoll. Übertreibt man es allerdings mit der Komplexität und der Änderungshäufigkeit, verleitet dies dazu, die Passwörter aufzuschreiben und am Arbeitsplatz zu hinterlegen.
- Backupstrategie: Einer der wichtigsten Punkte ist zweifellos die richtige Backupstrategie. Relevante Daten sollten möglichst umfassend und regelmässig auf räumlich getrennten Medien gesichert werden. Eine besondere Schwierigkeit stellt die Sicherung von Datenbanken dar. Hier ist es u. U. nicht möglich, geöffnete Dateien im laufenden Betrieb zu kopieren. Vielmehr muss die Sicherung aus der verwendeten Anwendung heraus oder mittels spezieller Software erfolgen.
- Virenschutz/Firewall: Ein aktueller Virenschutz gehört zu jedem IT-System. Ausserdem sollte, je nach Komplexität des Netzwerks, eine Firewall und ggf. ein Intrusion Detection System betrieben werden.

Backups sollte man automatisiert erstellen. Ansonsten ist die Gefahr gross, dass aus Zeitdruck, Bequemlichkeit oder Vergesslichkeit darauf verzichtet wird. Wichtige Daten sind inkrementell, also mit mehreren Versionsständen, abzulegen. Das heisst zunächst, dass nur geänderte Datensätze gesichert werden. Die älteren Versionen sollten aber möglichst noch für einen gewissen Zeitraum aufbewahrt werden, um Daten nach einem versehentlichen Löschen zu rekonstruieren.
Ein aktuelles Thema ist die Sicherung abgelegter Backups. Verschlüsselungstrojaner versuchen, jeglichen Speicher, auf den zugegriffen werden kann, zu kompromittieren. Befinden sich die Backups auf einem dauerhaft angebundenen Netzwerkspeicher oder auf externen Speichermedien, werden sie im schlimmsten Fall ebenfalls verschlüsselt. Hiervor schützt ein System, das normalen Nutzern den Zugriff verbietet, sowie das temporäre Einbinden der Speichermedien während der Sicherung.

1.2.4 Datenschutz

Personendaten sind nicht nur in materieller, sondern auch in ideeller Hinsicht ein wertvolles Gut, weil es in einer demokratischen und rechtsstaatlichen Gesellschaft nicht angeht, dass der Mensch nicht einmal mehr über eine minimale Kontrolle über die Verwendung von Daten, die ihn betreffen, verfügt. Das so genannte **informationelle Selbstbestimmungsrecht** bildet einen wichtigen Grundsatz unserer gesellschaftlichen Ordnung. D.h. jeder Mensch soll so weit wie nur möglich selbst darüber bestimmen können, welche Informationen über ihn wann, wo und wem bekannt gegeben werden. Das betrifft nicht nur die wirtschaftliche Seite; auch die staatlichen und gesundheitlichen Institutionen sind an Personendaten interessiert - man denke etwa an den Krieg gegen den internationalen Terrorismus oder gegen die organisierte Kriminalität, aber auch an die Anstrengungen, die Gesundheitskosten zu senken. Vereinfacht ausgedrückt könnte man sagen: Das erste Ziel des Datenschutzes muss sein, das informationelle Selbstbestimmungsrecht des Menschen zu verteidigen. Diese Aufgabe ist nicht immer einfach, da es zum Teil auch legitime Interessen geben kann, die dieses Selbstbestimmungsrecht einschränken, so etwa bei polizeilichen Ermittlungen.
Der Datenschutz soll gewährleisten, dass in jedem Fall die **Verhältnismässigkeit** beachtet wird, dass also immer nur so viele persönliche Daten wie nötig und so wenig persönliche Daten wie möglich gesammelt und bearbeitet werden, und dass man als betroffene Person auch die Möglichkeit hat, die Bearbeitung der Daten über sich so weit wie möglich zu kontrollieren und notfalls zu verhindern. Daher ist es unabdingbar, dass man als betroffene Person über die Möglichkeit verfügt, von den

Inhabern von Datensammlungen Rechenschaft darüber zu erhalten, welche Daten über einen bearbeitet werden. Zu diesem Zweck schreibt das Datenschutzgesetz ein **Auskunftsrecht** fest, das bei den Inhabern von Datensammlungen geltend gemacht werden kann.
Art. 13 der Bundesverfassung legt grundlegend fest, dass jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehr sowie auf Schutz vor Missbrauch ihrer persönlichen Daten hat.
Um diesen Schutz gesetzlich zu verankern, wurde das Bundesgesetz über den Datenschutz (DSG) verabschiedet, das seit dem 1. Juli 1993 in Kraft ist. Die entsprechende Verordnung (VDSG) regelt die Einzelheiten.
Neu (in Kraft ab September 2023) ist das **Bundesgesetz über den Datenschutz** (Datenschutzgesetz, DSG) vom 25. September 2020 (auch **nDSG** oder **revDSG** bezeichnet), zusammen mit der **Verordnung über den Datenschutz** (Datenschutzverordnung, **DSV**) vom 31. August 2022 und der **Verordnung über Datenschutzzertifizierungen** (**VDSZ**) vom 31. August 2022.
Ausserdem existieren auch in anderen Gesetzen und Bereichen zahlreiche Bestimmungen zum Schutz der Persönlichkeit. In den Artikeln 28-28l des Zivilgesetzbuches ZGB wird festgelegt, wie im Fall von Persönlichkeitsverletzungen rechtlich vorgegangen wird.Das Datenschutzgesetz (DSG) ist ein Rahmengesetz und erlaubt als solches einen grossen Spielraum bei der Beurteilung von Daten- und Persönlichkeitsschutzschutzverletzungen.

Es ist daher oft nicht möglich, umfassende allgemeine Aussagen zu machen.
Im Vordergrund steht in der Regel der Einzelfall, den es zu beurteilen gilt.
Einzelfall bedeutet hier nicht der individuelle Fall einer betroffenen Person, sondern bestimmte Datenbearbeitungen. Die Probleme, die sich bei einer solchen ergeben können, können technischer oder organisatorischer Natur sein

Privacy-By-Default und Privacy-By-Design spielen im neuen Datenschutzgesetz der Schweiz neu eine ganz besondere Rolle.

- Privacy-by-Default bezeichnet die Vorgabe, dass die tatsächlich verarbeiteten Personendaten mit dem Verwendungszweck in eindeutigem Einklang stehen müssen. Jegliche Nutzung zusätzlicher “vermeidbarer” Angaben erfordert die Inkenntnissetzung inklusive vorherige Zustimmung der Person.
- Privacy-by-Design umfasst eine Reihe von vorgegebenen Bearbeitungsgrundsätzen, die bereits bei der Aufnahme von Daten umgesetzt sein muss. Eine genaue interne Planung datenschutzrechtlicher Voreinstellungen ist essenziell und erspart Ihnen womöglich viel Ärger im Nachhinein.

Basic-Level

Expert-Level

Mit dem Begriff “Data Breach Notification” wird die erforderliche Massnahme bezeichnet, dass jegliche Datenverluste unverzüglich zu melden sind. Empfänger sind hierbei zum einen die Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Zum anderen müssen auch die jeweiligen Personen informiert werden, deren Daten betroffen sind. Letzteres jedoch nur im Falle, dass deren Persönlichkeits- oder Grundrechte in Gefahr sind.

Die Information der betroffenen Personen über bestimmte Mindestkriterien wird zukünftig als Pflicht eingeführt. Demnach müssen die Daten verarbeitenden Unternehmen mindestens die folgenden Punkte offenlegen:

- Die Identität sowie die Kontaktdaten der Verantwortlichen
- den Bearbeitungszweck
- die Empfänger beziehungsweise die Empfängerkategorie
- den gesonderte Hinweis auf eine mögliche automatische Datenerhebung
- Bei einer Weitergabe von Daten ins Ausland sollte die Einwilligung der betroffenen Person vorliegen beziehungsweise der Schritt vertragsrechtlich notwendig sein. Zusätzlich nachgewiesen werden können, dass auch im Zielland alle datenschutzrechtlich notwendigen Bestimmungen eingehalten werden. (vgl. auch Unterkapitel Cloudcomputing 3.2).

Als eine der letzten besonders wichtigen Neuerungen im revidierten DSG sind Datenschutzfolgenabschätzungen zu nennen. Diese werden Pflichtbestandteil im Falle besonders risikoreicher Datenverarbeitungen. Hierbei übernehmen die Verantwortlichen die Vorkalkulation der möglicherweise entstehenden Risiken sowie auch Massnahmen zur Reduzierung dieser. Ziel ist, zusammenhängende Gefahren auf ein Minimum zu reduzieren – und das im Zweifel auch nachweisen zu können.

1.2.5 Weitere Informationen

Videos

- Das neue Datenschutzgesetz der Schweiz - YouTube

Dokumente und Links

- Das neue Datenschutzgesetz aus Sicht des EDÖB
- Datenschutz (admin.ch)
- Das neue Schweizer Datenschutzgesetz (revDSG) auf einer DIN-A4-Seite (s. Beilage PDF oder Link)

1.2.6 Archivieren

Basic-Level

Das Archivieren aktuell nicht mehr benötigter Daten gehört ebenfalls zu den Aufgaben des Datenmanagements. Dies betrifft diejenigen, für die es eine gesetzliche Pflicht zur Aufbewahrung gibt, etwa bei Rechnungen und Steuerunterlagen. Daher sollte dieser Aspekt Bestandteil eines Datenmanagement-Konzepts sein.
Separates Speichern kann vorteilhaft sein. So vermindert man das Volumen aktueller Datensicherungen und der Datenschutz lässt sich gewährleisten. Zu beachten ist, dass nicht alle Speichermedien für eine Archivierung geeignet sind. Festplatten sollten beispielsweise regelmässig eingeschaltet werden, um die Funktionstüchtigkeit zu garantieren. Optische Datenträger wie CDs sind empfindlich gegenüber äusseren Einflüssen und haben ohnehin nur eine begrenzte Lebensdauer. Optimal sind Bandlaufwerke mit Magnetbändern. Nachteilig hierbei sind jedoch die hohen Anschaffungskosten für Laufwerke und die umständliche Handhabung. Vorteilhaft wiederum sind die günstigen Preise für Sicherungsbänder und die lange Haltbarkeit.

1.2.7 Löschen

Nicht mehr benötigte Daten sollten gelöscht werden. So ist man auch gleich die

Verantwortung für deren Sicherheit los. Daher sollte ein Datenmanagement-Konzept vorsehen, dass solche Daten selektierbar und separat löschbar sind. Vor allem personenbezogene Daten sollten sicher gelöscht werden.
Ein Löschen mit Betriebssystemfunktionen führt üblicherweise nur dazu, dass die Daten zum Überschreiben freigegeben werden. Tatsächlich existieren sie noch auf der Festplatte, bis der Speicherplatz zufällig benötigt wird und sie überschrieben werden. Sicheres Löschen ist heutzutage nicht mehr so einfach. Normale (magnetische) Festplatten können mittels entsprechender Software komplett überschrieben werden („Wipen“). Dabei wird der gesamte Speicher einmal oder mehrmals mit Nullen oder Zufallswerten beschrieben. Viele Festplatten verwenden inzwischen jedoch Flashspeicher. Da diese weniger langlebig sind, beinhalten sie Reservebereiche, auf die der Nutzer nicht zugreifen kann. Dementsprechend können sie auch nicht überschrieben werden. Hier hilft oft nur die Zerstörung des Speichers. Deshalb ist es sinnvoll, den Speicher vollständig zu verschlüsseln. Dann werden zu keinem Zeitpunkt Daten im Klartext auf der Festplatte abgelegt und die Entsorgung ist unproblematisch.

Basic-Level

1.3 Zusammenspiel zwischen Datenschutz, gesetzlichen Aufbewahrungs- und Verjährungsfristen

1.3.1 Aufbewahrungsdauer

Expert-Level

Personendaten können nur für eine gewisse Dauer aufbewahrt werden. Danach sind sie nach schweizerischem wie auch nach europäischem Datenschutzrecht zu löschen. Ausgenommen von der Löschpflicht sind zunächst Daten, die aufgrund einer gesetzlichen Vorschrift aufbewahrt werden müssen. Ist das der Fall, müssen und dürfen Dokumente während dieser Dauer nicht gelöscht werden. Am wichtigsten ist die gesetzliche Aufbewahrungspflicht für Geschäftsbücher, Geschäftsberichte und Buchungsbelege, die 10 Jahre beträgt.

Für die Zeit nach Ablauf dieser Dauer oder falls keine gesetzliche Aufbewahrungsfrist besteht, können Dokumente zunächst so lange verwendet und aufbewahrt werden, wie die darin enthaltenen Personendaten zum Zweck, zu dem sie erhoben wurden, noch gebraucht werden. Auch aus dem Grundsatz der Datenrichtigkeit für Personendaten wird die Pflicht zur Löschung abgeleitet: Je älter Personendaten sind, desto eher werden sie in der Tendenz nicht mehr zutreffen.

Beispielsweise können Unterlagen, die für das Verfassen eines Zwischenzeugnisses benötigt werden, solange behalten werden, wie das Anstellungsverhältnis dauert. Grundlagendokumente des Unternehmens, wie etwa dessen Statuten oder Organisationsreglement, sollten während der ganzen Lebensdauer des Unternehmens aufbewahrt werden.

Werden Personendaten nicht mehr zum ursprünglich erhobenen Zweck gebraucht, kann im Allgemeinen angenommen werden, dass zu Beweiszwecken Unterlagen dennoch so lange aufbewahrt werden dürfen (aber nicht müssen) bis die Verjährungsfrist der zugrundeliegenden Forderung noch nicht abgelaufen ist. Ab diesem Zeitpunkt kann eine Forderung nicht mehr (gerichtlich) durchgesetzt werden. Beispielsweise verjährt die Forderung aus einem Auftragsverhältnis auf Bezahlung eines Übersetzungshonorars 10 Jahre nach seiner Fälligkeit. Hat der Kunde dem Übersetzungsunternehmen die Rechnung nicht bezahlt, kann das Unternehmen dies vom Kunden noch während 10 Jahren nach Bestellung der Übersetzungsleistung verlangen (und auch durchsetzen), später, aber nicht mehr. Bei der Frage, welche Unterlagen während laufender Verjährungsfrist noch zu behalten sind, geht es im Wesentlichen um die Einschätzung, wie das Unternehmen im Hinblick auf potenzielle rechtliche Auseinandersetzungen aufgestellt sein will.

Zusammengefasst lässt sich die Aufbewahrungsdauer von Personendaten enthaltenden Dokumenten anhand dieser drei Fragen nachvollziehen (in dieser Reihenfolge):

- Besteht eine gesetzliche Aufbewahrungsfrist?
- Werden Personendaten noch gebraucht?
- Wenn nicht: ist eine weitere Aufbewahrung zu Beweiszwecken bis zum Ablauf der Verjährungsfristen erforderlich?

Wenn alle drei Fragen mit nein beantwortet werden können, verlangt der Datenschutz, dass Personendaten gelöscht werden oder der Zugriff darauf zumindest stark eingeschränkt wird. Da die gesetzliche Aufbewahrungspflicht für Geschäftsbücher, Geschäftsbericht und Buchungsbelege 10 Jahre beträgt und viele Forderungen nach 10 Jahren verjähren, haben sich als genereller Richtwert 10 Jahre eingebürgert.

Als Faustregel wird in der Praxis auch bei Patientendossiers auf die allgemeine Verjährungsfrist von zehn Jahren abgestellt. In Einzelfällen kann aber auch eine kürzere oder längere Aufbewahrungsfrist vorgesehen werden. In einigen Kantonen sehen die kantonalen Gesundheitsgesetze genaue Aufbewahrungsfristen vor.

Es gelten aber auch andere gesetzliche Aufbewahrungs- und Verjährungsfristen (vgl. Wie lange dürfen Personendaten gespeichert werden? 05/2019 – Fachartikel Swiss Infosec AG)

Dokumente	Verjährungsfrist
Dokumente mit Bezug zu sämtlichen Forderungen, für die keine Spezialregelung gilt (vgl. dafür nachfolgende Zeilen)	10 Jahre nach Fälligkeit Forderung
Dokumente mit Bezug zu folgenden Forderungen: • Mietzins, Versicherungsprämien und andere regelmässige zu bezahlende Leistungen • Leistungen von Handwerkern • Konsumentenverhältnis • Arbeitslohn	5 Jahre nach Fälligkeit Forderung/Ablauf regelmässiger Leistungen

Tabelle 1Aufbewahrungsfristen

1.3.2 Verjährungsfristen

Wir empfehlen deshalb: Legen Sie unter Berücksichtigung des Bearbeitungszwecks und der jeweils geltenden Aufbewahrungs- und Verjährungsfristen für die Dokumente, die Personendaten enthalten, Fristen fest, nach deren Ablauf die Personendaten gelöscht werden können.

1.3.3 Sonstige rechtliche Vorgaben

Neben den Bestimmungen aus dem Datenschutzgesetz gibt es weitere Regeln, die Unternehmen zum Datenschutz verpflichten. Werden Versäumnisse festgestellt, die zu einem Missbrauch personenbezogener Daten führen, können Inhaber oder Beauftragte **haftbar gemacht werden**.

1.4 Herausforderungen des Datenmanagements

Datenmanagement ist ein dynamischer Prozess und muss immer wieder an aktuelle Erfordernisse angepasst werden. Dabei entstehen jeweils neue Herausforderungen.

1.4.1 Big Data

Datenmengen nehmen stetig zu. Folglich gibt es hohe Anforderungen an die Skalierbarkeit von Speichern und Backup-Kapazitäten sowie die Ordnung und Auffindbarkeit benötigter Daten. Je mehr Daten man erheben kann, umso wichtiger wird zudem der Punkt Datensparsamkeit. Das Herausfiltern von wichtigen Informationen sollte deshalb mehr und mehr im Fokus stehen.

1.4.2 Sicherheit

Verantwortliche von Netzwerkverbünden sehen sich immer neuen Gefahren ausgesetzt. Informationsdiebstahl durch Social Engineering und Sabotage durch Verschlüsselungstrojaner sind nur einige der Szenarien. Je mehr ein Unternehmen seinen Datenbestand digitalisiert, desto abhängiger wird es von der Funktionsfähigkeit des verwendeten Systems. Deshalb gilt es, sich permanent über neue Risiken zu informieren und Vorsorge für den Ausfall von Hardware oder einen fehlenden Zugriff auf die eigenen Systeme zu treffen.

2 Anonymisierung und Pseudonymisierung

Expert-Level

Pseudonymisierung ist ein Vorgang der Datenverarbeitung und soll verhindern, dass Personen in einer Datensammlung durch Merkmale eindeutig identifizierbar sind. Hierfür ersetzt die Pseudonymisierung Identifikationsmerkmale wie Namen mit anderen Kennzeichen wie Schlüsseln oder Pseudonymen. Die grundsätzliche Zuordnungsvorschrift bleibt in den pseudonymen Daten nach der Pseudonymisierung erhalten, ist aber ausgelagert. Beispielsweise wird eine externe Datei gepflegt, in der die jeweiligen Schlüssel oder Pseudonyme und die zugehörigen Namen gespeichert sind. Auf diese Daten kann nur unter bestimmten Voraussetzungen und nur von einem definierten Personenkreis zugegriffen werden. So kann es zur Erfüllung gesetzlicher Verpflichtungen notwendig werden, auf Verlangen die Zuordnung zu einer bestimmten Person vorzunehmen.
Der Vorgang der Pseudonymisierung ist also grundsätzlich umkehrbar.
Die Pseudonymisierung unterscheidet sich deutlich von der **Anonymisierung**.
Pseudonyme Daten gelten weiterhin als personenbezogene Daten. Zahlreiche Vorgaben im Umgang mit den Daten sind zu beachten. **Im Gegensatz zu nicht pseudonymisierten Daten ist der technisch-organisatorische Schutzbedarf jedoch geringer.** Das Pseudonymisieren der Daten selbst ist ein Verarbeitungsvorgang personenbezogener Daten und hat alle gesetzlichen und datenschutzrechtlichen Vorgaben zu erfüllen.

2.1 Abgrenzung zwischen Anonymisierung und Pseudonymisierung

Im Umfeld der Pseudonymisierung fällt häufig der Begriff Anonymisierung. Beides sind Verfahren zum Schutz der Privatsphäre und der personenbezogenen Daten. Je nach Situation und Ziel der Datenverarbeitung sind Anonymisierung oder Pseudonymisierung geeignete Techniken, um bestimmte Anforderungen des Datenschutzes zu erfüllen. Die Anonymisierung unterscheidet sich von der Pseudonymisierung und erzeugt vollständig anonymen Daten.
Der Unterschied zwischen der Anonymisierung und der Pseudonymisierung besteht darin, dass bei der Pseudonymisierung eine grundsätzliche Zuordnungsmöglichkeit der Daten zu bestimmten Personen bestehen bleibt. Allerdings ist diese ausgelagert und auf konkrete Verantwortungsbereiche beschränkt. Bei anonymen Daten ist keinerlei Zuordnungsmöglichkeit mehr gegeben. In pseudonymen Daten bleiben die Bezüge der Datensätze grundsätzlich bestehen, allerdings werden sie durch Schlüssel oder Pseudonyme für die eigentlichen Nutzer der Daten anonymisiert. Die Identifikationsmerkmale und Daten sind praktisch voneinander getrennt und nur unter definierten Voraussetzungen zugänglich.
Während der Vorgang der Pseudonymisierung umkehrbar ist und eindeutige Identifikationsmerkmale der Personen wieder herstellbar sind, verlieren anonymisierte Daten diese eindeutigen Identifikationsmerkmale und der Vorgang der Anonymisierung ist nicht umkehrbar oder nur mit unverhältnismässig grossem Aufwand realisierbar.
Viele Grundsätze des Datenschutzes gelten für vollständig anonyme Daten nicht mehr.

2.2 Was sind pseudonyme Daten?

Die Pseudonymisierung generiert pseudonyme Daten. Pseudonyme Daten lassen sich keiner spezifischen Person mehr zuordnen. Um Personen eindeutig zu identifizieren, sind externe Zuordnungsvorschriften hinzuzuziehen, die ausgelagert gespeichert sind. Die grundsätzliche Möglichkeit der Zuordnung besteht nur durch Zuhilfenahme dieser Zuordnungsregeln.

2.3 Ansätze zur Anonymisierung und Pseudonymisierung

Sowohl bei der Anonymisierung als auch bei der Pseudonymisierung müssen identifizierende Merkmale so gelöscht (bei Anonymisierung) oder von den anderen personenbezogenen Daten getrennt (bei Pseudonymisierung) getrennt werden, dass ein Rückschluss auf die Person bzw. deren schutzwürdige Daten wesentlich erschwert wird.
Hierzu genügt es in der Regel nicht, nur die Merkmale zu entfernen, die direkt auf die Person rückschliessen lassen.
Beispiele dafür wären der Name, der genaue Wohnort, die E-Mail, Telefonnummer oder das Geburtsdatum. Meist ist es zusätzlich erforderlich, Daten zu verfälschen, zu verändern oder zu gruppieren:

- Wohnort (inklusive Strasse und Hausnummer) durch Postleitzahl oder sogar nur erste Ziffern der Postleitzahl ersetzen
- Geburtsdatum auf Jahreszahl oder sogar grösseres Intervall (z.B. fünf Jahre) limitieren
- Bei hierarchischen Kodiersystemen (Taxonomien wie der ICD-Diagnosekatalog) Werte auf höhere Hierarchieebene reduzieren
- Einzelwerte zu kombiniertem Wert zusammenfassen. Beispielsweise könnte man Leberwerte wie Gamma-GT, GOT oder GPT zusammenfassen in „erhöhte Leberwerte“ und „unauffällige Leberwerte“
- Zeitliche und räumliche Bezüge entfernen oder abstrakter gestalten. Beispielsweise konnten bei einer vermeintlich anonymisierten Datensammlung Personen identifiziert werden, weil es nur wenige Menschen gab, die zu bestimmten Zeitpunkten von einem zum anderen Ort umzogen
- Werte oder Datensätze entfernen

Die Pseudonymisierung personenbezogener Daten wird mithilfe verschiedener Verfahren vorgenommen. In der Regel werden eindeutige Identifikationsmerkmale wie Namen durch Pseudonyme, eindeutige Codes, IDs oder Schlüssel ersetzt. Die Zuordnung der Pseudonyme, Codes, IDs oder Schlüssel zum Namen wird in einer zusätzlichen Tabelle gepflegt und technisch oder organisatorisch getrennt von den pseudonymisierten Daten aufbewahrt.

2.4 Beispiele für die Pseudonymisierung

Beispiel für die Pseudonymisierung ist das Ersetzen der Namen der Mitarbeiter in Unternehmensdaten durch eine Personalnummer. Im Datensatz selbst besteht keine eindeutige Zuordnungsmöglichkeit mehr zur Identität des Mitarbeiters. Nur unter Zuhilfenahme einer Zuordnungstabelle mit Personalnummer und Name, auf die bestimmte Personen im Unternehmen Zugriff haben, kann der Mitarbeiter eindeutig identifiziert werden.
Weitere Beispiele sind die Verwendung von Nicknames oder E-Mail-Adressen ohne Bezug auf den realen Namen. Für Aussenstehende ist nicht erkennbar, welche Person sich hinter einem Nickname oder einer E-Mailadresse verbirgt. Für den Betreiber der Webseite oder des E-Mail-Services lassen sich die Bezüge zu realen Personen durch Zuhilfenahme der dort vorhandenen Registrierungsinformationen wieder herstellen.
Möchte ein Professor in einer Hochschule die Ergebnisse einer (schriftlichen) Prüfung den Studenten einfach zugänglich machen, so bittet er diese darum, während der Prüfung ein selbstgewähltes Pseudonym auf den Blättern zu notieren. Nach der

Expert-Level

Korrektur kann der Professor einen Aushang (ggf. auch im Internet) veröffentlichen, in dem alle Ergebnisse nach dem Schema <Pseudonym> <Note> aufgeführt werden. Somit ist die Zuordnung des Pseudonyms zum jeweiligen Studenten nur durch den Professor oder im Einzelfall durch den Studenten herzustellen. Würden in diesem Beispiel im Nachhinein die Prüfungsblätter mit den von den Studenten notierten Pseudonymen zerstört werden, so wären die Angaben auf dem Notenaushang für die Allgemeinheit anonymisiert, da keine Zuordnung zu den jeweiligen Studenten mehr möglich wäre. Jeder Student wird jedoch, da er sich sein Pseudonym gemerkt hat, seinen Eintrag auf dem Notenaushang wiedererkennen können.
Eine geheime Abstimmung bei Wahlen beruht auf dem Prinzip der Anonymisierung (vgl. Wahlgeheimnis). Es ist zwar noch nachvollziehbar, wer gewählt hat, aber eine Zuordnung zwischen Wahlzettel und Wähler ist nicht mehr möglich.
Im medizinischen Umfeld wird ebenfalls häufig mit pseudonymisierten Daten gearbeitet. So bleiben Personen bei statistischen Auswertungen geschützt, lassen sich aber bei Vorliegen eines wichtigen Grundes durch einen definierten Verantwortungskreis wieder identifizieren. Ein weiteres Beispiel ist die öffentliche Bekanntgabe von Prüfungsergebnissen mit Zuordnung zu einem Pseudonym. Nur wer das Pseudonym kennt, in der Regel die prüfende Organisation oder der Prüfling, kann nachvollziehen, für welche konkrete Person das Prüfungsergebnis Gültigkeit hat.

2.5 Unzureichende Pseudonymisierung

Daten in Form eines Diagnose-Codes und einer Postleitzahl, die über eine pseudonymisierte Patienten-ID verknüpft sind, betrachtet man in der Regel als ausreichend pseudonymisiert. Wenn die PLZ jedoch ein 2000-Einwohnerdorf repräsentiert und die Diagnose ausreichend selten ist (z.B. Down-Syndrom), kann die Zuordnung gelingen.

2.6 De-Anonymisierung mit Hilfe weiterer Daten

Regelmässig übersieht man die Tatsache, dass es neben den eigenen pseudonymisierten Daten weitere Daten gibt, die in Kombination mit den eigenen Daten eine De-Anonymisierung erleichtern. Hier sind insbesondere öffentliche Daten wie solche aus sozialen Netzwerken zu betrachten.
Die US-Wissenschaftlerin Latanya Sweeney zeigte zum Beispiel (Sweeney_Article.pdf (epic.org)), dass sich über die Kombination von Postleitzahl, Geburtsdatum und Geschlecht ungefähr 87 Prozent aller US-Amerikaner eindeutig identifizieren lassen – ganz ohne Namen. Sweeney etwa kombinierte öffentlich zugängliche Krankenversicherungsdaten, die vermeintlich anonymisiert worden waren, mit einem Wählerverzeichnis, das für 20 Dollar frei erhältlich war. Postleitzahl, Geburtsdatum und Geschlecht fanden sich in beiden Datensätzen. Man nennt solche Gruppen von Merkmalen, über die sich Datensätze miteinander verknüpfen lassen, Quasi-Identifizierer (QI). Sweeney konnte darüber einen kombinierten Datensatz erstellen: Das Wählerverzeichnis steuerte die Namen bei, die Versicherungsdaten die zugehörigen Erkrankungen. Die Zuordnung geschah über Postleitzahl, Geburtsdatum und Geschlecht. Dadurch fand Sweeney beispielsweise Diagnosen und Behandlungen des damaligen Gouverneurs von Massachusetts heraus.

2.7 k-Anonymität: Wie man Daten richtig anonymisiert

Mit Hilfe der k-Anonymität gelingt es, den Grad der Anonymisierung bzw. Pseudonymisierung zu bewerten
Ein Datensatz ist k-anonym, wenn es zu jedem Eintrag mindestens k − 1 weitere Einträge mit identischen QI-Werten gibt. Ein Vergleich mit anderen Datensätzen, wie einem Wählerverzeichnis, hilft dann nicht, weil man keinen Eintrag mehr individuell zuordnen kann, sondern immer mindestens k passende Einträge findet – oder gar keinen.

Die zentrale Frage ist, was die QIs eines Datensatzes sind. Allgemein entscheiden lässt sich das nicht, was eine der Schwächen von k-Anonymität ist. Ob eine Merkmalskombination als QI betrachtet werden muss, hängt davon ab, welche anderen Datensätze einem Angreifer, der die Anonymisierung aufheben will, zur Verfügung stehen. (vgl. k-Anonymität | heise online).
Dazu ein Beispiel: Stellen Sie sich vor, Sie sind Dozent an einer Hochschule. Für eines Ihrer Seminare erstellen Sie eine Tabelle, in der Sie für jeden teilnehmenden Studenten Name, Studiengang, Fachsemester, Anwesenheitsquote und Note festhalten. Die folgende Infografik zeigt dieses Beispiel in der ersten Tabelle ganz oben. Nachdem Sie die Tabelle erstellt haben, würden Sie den Datensatz gerne zum Vergleich mit Kollegen teilen. Weil Anwesenheitsquote und Noten schützenswerte Daten sind, möchten Sie den Datensatz k-anonymisieren.

Expert-Level

Abbildung 1 k-anonymisieren

Dazu müssen Sie zuerst festlegen, was die QIs sind: Natürlich ist der Name identifizierend und daher schon für sich allein ein QI. Aber auch Wertekombinationen für Studiengang und Semester sind – in einem kleinen Seminar – eindeutig. Zudem tauchen Studiengang und Fachsemesterzahl auch in anderen Datensätzen auf, oft sogar zusammen mit Namen von Studenten. Daher bilden Studiengang und Semesterzahl ebenfalls einen QI. Problematisch ist die protokollierte Anwesenheit: Im Beispiel ist sie der Einfachheit halber nicht an QIs beteiligt. Jedoch kann man nicht ausschliessen, dass Teilnehmer des Seminars darüber Buch geführt haben, wer wann anwesend war. Eine solche Liste würde Anwesenheit und Namen kombinieren, wodurch das Merkmal "Anwesenheit" ebenfalls für QIs in Betracht gezogen werden müsste.

2.8 Methoden zur Anonymisierung

Hat man die QIs identifiziert, muss man die betroffenen Werte so bearbeiten, dass der Datensatz k-anonym wird. Dafür gibt es zwei grundsätzliche Werkzeuge: Generalisierung und Unterdrückung. Bei der Generalisierung vergröbert man die Werte eines Merkmals, damit sie in grösseren Gruppen zusammenfallen. Statt der exakten Angabe eines Datums genügt es beispielsweise oftmals, wenn nur der Monat oder das Jahr bekannt gegeben wird. Zahlen lassen sich runden oder in Bereiche einteilen. Bestimmte Werte lassen sich über eine Hierarchie auf abstraktere Begriffe abbilden. Manche Werte, wie Namens- oder Geschlechtsangaben, lassen sich allerdings nur sinnvoll generalisieren, indem man alle Einträge in einer Spalte auf denselben Wert setzt, also praktisch die Spalte löscht.

Man nennt eine Generalisierung "global", wenn sie alle Werte eines Attributs betrifft. Alternativ lassen sich lediglich diejenigen Werte eines Attributs generalisieren, für die es tatsächlich nötig ist, um k-Anonymität zu erreichen. Durch so eine lokale Generalisierung wird der Datensatz zwar weniger einheitlich, verliert jedoch auch weniger Genauigkeit. Die Generalisierung in Schritt 3 des Beispiels in Abbildung 1 k-anonymisieren ist global. Stattdessen hätte man aber auch nur die Werte der Zeilen 4 und 5 auf "Ingenieurswissenschaften" generalisieren können. Der Anonymisierungseffekt wäre der gleiche.

Wenn nur noch einzelne Spezialfälle in einem Datensatz verhindern, dass er k-anonym ist, dann bietet es sich an, diese Fälle einfach zu löschen. Man unterdrückt also einzelne Zeilen in der Tabelle. Dadurch wird der Datensatz allerdings verfälscht, weshalb man lediglich eine begrenzte Anzahl solcher Ausreisser unterdrücken sollte. Sind es zu viele, ist es besser, weiter zu generalisieren.

2.9 Notwendige Anonymität

Es gibt verschiedene Strategien und Algorithmen, mit denen man Datensätze k-anonymisiert. Sie unterscheiden sich hauptsächlich darin, wo und in welcher Reihenfolge sie generalisieren und unterdrücken. Oft wird auch eine maximale Anzahl von Zeilenunterdrückungen vorgegeben, damit man tatsächlich nur Ausreisser und keine relevanten Teilmengen des Datensatzes löscht. Optimale k-Anonymisierung zu erreichen, ist schwierig und obendrein abhängig vom Nutzen, den Empfänger mit den Daten erzielen wollen. Es gilt, einen Kompromiss zu finden, der eine möglichst gute Anonymität gewährleistet, aber für den vorgesehenen Forschungszweck noch genügend auswertbare Informationen enthält.

Je grösser man k wählt, desto anonymer ist ein Datensatz. Damit sinkt aber auch sein Nutzwert, denn um hohe k-Werte zu erreichen, muss üblicherweise mehr und gröber generalisiert werden. In der Regel wird k deshalb abhängig von der Situation, dem betroffenen Datensatz und dem angenommenen Angriffsszenario gewählt. Wenn der betroffene Datensatz nur einige Dutzend Einträge umfasst, beschränkt man sich oft auf kleine k-Werte von 10 bis 15. Grössere Werte sind bei kleinen Studien kaum möglich, ohne den Datensatz so stark zu generalisieren, dass er wertlos wird.

Anonymisierungswerkzeuge wie das Open-Source-Tool ARX unterstützen k-Anonymität. QIs, Generalisierungsschritte und so weiter lassen sich einstellen und ausprobieren. Auch bei der Nutzen- und Risikoanalyse hilft das Werkzeug.

2.10 Weitere Informationen

Anonymisierung personenbezogener Daten -Ein branchenübergreifender Praxisleitfaden für Industrieunternehmen

Expert-Level

3 Anwendungsbereiche Datenmanagement und Datenschutz

3.1 IoT und Datenschutz

Das Internet der Dinge (IoT) beschreibt das Konzept der gezielten Vernetzung von physischen Gegenständen mit dem Internet. Die Geräte kommunizieren miteinander und mit ihren Nutzern, arbeiten selbstständig und bedürfen keiner regelmässigen Kontrolle durch die Nutzer. Präzise Daten in grossen Mengen werden erhoben und in Echtzeit analysiert. Kombiniert mit KI-Anwendungen ergeben sich breite und mächtige Anwendungsfelder für Unternehmen nahezu jeder Grösse und Branche.

Basic-Level

Längst hat das IoT nahezu all unsere Lebensbereiche durchdrungen, ist weder aus der Welt der Industrie 4.0 noch aus unserem persönlichen Alltag in Privathaushalten mehr wegzudenken. Um die typischerweise zur Veranschaulichung der Möglichkeiten des IoT herangezogenen Paradebeispiele des autonomen Fahrens, der Smart City oder der Personalisierung und Optimierung der Gesundheitsversorgung zu realisieren, ist das IoT auf riesige Mengen an Daten angewiesen.
Da es sich bei diesen Daten oft um personenbezogene Daten handelt, stellen das IoT und seine Anwendungen Herausforderungen an den Datenschutz und das informationelle Selbstbestimmungsrecht von Personen. In dieser Hinsicht sei an die breite öffentliche Diskussion erinnert, die darüber geführt wurde, dass Wearables wie Smart Watches und Fitnesstracker Gesundheitsdaten erheben. Intensiv diskutiert wurde auch die Notwendigkeit zur flächendeckenden Ausstattung des öffentlichen Raums mit bewegungssensitiven Sensoren, um autonomes Fahren zu ermöglichen.
Die Datenschutzgesetzgebung greift also auch im Bereich des Internets der Dinge. Sie greift im Zusammenhang mit IoT-Anwendungen aber selbstverständlich nur dann, wenn diese Anwendung überhaupt personenbezogene Daten (Personendaten) verarbeitet. In folgenden Fällen liegt z.B. eine solche Personenbeziehbarkeit bei Anwendungen des Internet of Things vor:

- Akustische, optische oder biometrische Sensoren, die personenbezogene Daten verarbeiten, kommen zur Anwendung.
- Der Einsatzort eines Sensors ermöglicht es, Rückschlüsse auf die Gewohnheiten einer Person abzuleiten (z. B. Bewegungssensoren).
- Ein Personenbezug entsteht, sobald sich ein Nutzer mit Namen oder anderen Identifikationsmerkmalen anmeldet, um die IoT-Anwendung nutzen oder steuern zu können.
- Kommuniziert ein Nutzer mit einer IoT-Anwendung, können beispielsweise die Verarbeitung von IP-Adressen oder die Auswertung von MAC-Adressen zur Anwesenheitserkennung zur Personenbeziehbarkeit führen.

Unternehmen sollten beim Einsatz von IoT-Anwendungen darauf achten, dass die Sensoren nicht mehr Daten erheben als zur Erfüllung des wirtschaftlichen Zwecks unbedingt notwendig. Die Prinzipien der Datensparsamkeit und der Zweckbindung sind einzuhalten. Die Verwendung anonymisierter Daten ist nur dann statthaft, wenn es sich um eine echte Anonymisierung handelt, sprich, wenn aus der Kombination verschiedener anonymisierter Datensätze keinerlei Rückschlüsse auf einzelne Personen mehr möglich sind.

3.1.1 Bestimmung des datenschutzrechtlich Verantwortlichen

Verantwortlich für den Datenschutz könnten z.B. der Hersteller, Geräteverleiher oder dritte Dienstanbieter sein. Wird ein Dritter involviert, ist eine Einwilligung des Nutzers in die Weitergabe seiner Daten oder eine andere Rechtsgrundlage unabdingbar. Grundsätzlich ist datenschutzrechtlich

die Stelle verantwortlich, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

3.1.2 Rechtsgrundlage für die Datenverarbeitung

Mit Anwendung der DSV gilt, dass die Erhebung, Verarbeitung und Speicherung personenbezogener Daten grundsätzlich verboten sind, wenn es dafür keine gesetzliche Grundlage gibt bzw. die betroffene Person nicht eingewilligt hat. Sofern eine Datenverarbeitung in den Anwendungsbereich der DSV fällt, kommen mehrere Rechtsgrundlagen für diese Datenverarbeitung in Betracht.
Dabei kann sich gerade für IoT-Anwendungen das rechtssichere Einholen von Einwilligungen schwierig gestalten. Dazu gehört insbesondere, dass die Hersteller über Funktionen und Datenflüsse in verständlicher Form aufklären. Bei vielen IoT-Lösungen ist es indes technisch schon gar nicht möglich, eine Einwilligung anzufordern oder zu erteilen. Zudem muss der Betroffene diese jederzeit widerrufen können. Es ist oft aber gar nicht möglich, der Datenverarbeitung als Nutzer der IoT zu widersprechen.
Daneben gibt es die Möglichkeit der Rechtmässigkeit der Datenverarbeitung, wenn die Datenverarbeitung für die Durchführung eines Vertragsverhältnisses notwendig ist oder der Verarbeiter ein berechtigtes Interesse an der Nutzung der Sensoren hat. Das sollte vor der Anwendung geprüft und diese Prüfung dokumentiert werden. Jede Anwendung muss hier im konkreten Kontext genau betrachtet werden.

3.1.3 Informationspflichten und Datenschutzrechte

Unabhängig von der Rechtsgrundlage der Datenverarbeitung sind unbedingt die Informationsrechte der betroffenen Personen zu beachten. So muss einer betroffenen Person eine Vielzahl an Informationen bei der Datenerhebung mitgeteilt werden. Ausnahmsweise besteht keine Informationspflicht, wenn die Erteilung der Information einen unverhältnismässigen Aufwand bedeuten würde. Dies aber nur, wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden. IoT-Anbieter benötigen also zwingend ein Konzept zur Umsetzung der Informationspflichten.

3.1.4 Privacy by Design und by Default

Die europäische und die schweizerische Gesetzgebung enthalten Vorschriften zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Privacy by Design und by Default). Betreiber von IoT-Anwendungen sind somit dazu verpflichtet ein datenschutzkompatibles und datenschutzfreundliches IoT-Design zu entwickeln. Oft fallen die Hersteller einzelner Komponenten jedoch nicht unter die Regelungen, da sie die Komponenten nicht selbst betreiben. In Praxis erhalten dann die letztendlichen Betreiber von IoT-Anwendungen häufig unsichere oder schlecht konfigurierbare Komponenten, für deren Einsatz sie datenschutzrechtlich einzustehen haben.

3.1.5 Datenschutzfolgenabschätzung (DSFA)

IoT kann zudem die Voraussetzungen für die in besonderen Fällen geforderte Datenschutzfolgenabschätzung (DSFA) erfüllen. Hat eine Verarbeitung von personenbezogenen Daten aufgrund der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, muss der Verantwortliche eine DSFA durchführen. Eine DSFA bietet die Möglichkeit, Sicherheitslücken frühzeitig zu erkennen und adäquate Massnahmen zur Erhöhung der Datensicherheit zu implementieren. Hierbei handelt es sich allerdings nicht um ein einmaliges Verfahren, sondern um einen kontinuierlichen Prozess. Ändern sich Details eines Datenverarbeitungsvorganges, kann eine erneute Prüfung erforderlich sein.

3.1.6 Grundsätze der Datensparsamkeit und der Zweckbindung

Unternehmen sollten beim Einsatz von IoT-Anwendungen ihr Augenmerk darauf richten, dass ihre Sensoren nicht mehr Daten erheben als zur Erfüllung des Zwecks der Komponente unbedingt notwendig sind (Zweckbindung).
Nach der DSV sind die Prinzipien der Datensparsamkeit und der Zweckbindung einzuhalten. Nach den Prinzipien der Datensparsamkeit und der Zweckbindung ist die Verwendung anonymisierter Daten insbesondere nur dann erlaubt, wenn es sich um eine echte Anonymisierung handelt. Oft werden

Daten als „anonym“ bezeichnet, sind es aus DSGVO-Sicht aber keineswegs, weil andere miterhobene Informationen eine Identifikation weiterhin ermöglichen. Daten sind nur dann anonym, wenn aus der Kombination verschiedener anonymisierter Datensätze keinerlei Rückschlüsse auf einzelne Personen möglich sind.

3.1.7 Datenkontrolle für die Nutzer

Die Hoheit über die verarbeiteten Daten sollte bei den Nutzern liegen. Es muss ihnen ermöglicht werden, einzelne Funktionen der Datenverarbeitung zu erkennen und ggf. abschalten zu können.

3.1.8 Technisch-organisatorische Schutzmassnahmen, insbesondere Verschlüsselung

Idealerweise verschlüsseln IoT-Unternehmen alle Daten, die durch ihre Geräte erfasst und zur Analyse genutzt werden und ergreifen weitere IT Security Massnahmen (IoT Sicherheit zum Schutz der Vertraulichkeit und Integrität der Daten. Der erste Schritt bei der Suche nach einer besseren, passenden IoT-Sicherheit ist die Risikoanalyse.

Expert-Level

- Hier bietet die EU-Agentur für Netz- und Informationssicherheit ENISA ihre Hilfe an.
  Die ENISA veröffentlichte ein Online-Tool, das die Betreiber von IoT bei der Risikobewertung unterstützen soll, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT . Das Tool bietet eine kombinierte Sicht auf die bewährten Sicherheitsmethoden. Die durch dieses Tool bereitgestellten Informationen für jeden Themenbereich spiegeln die Informationen wider, die in entsprechenden ENISA-Berichten enthalten sind, die in der Vergangenheit veröffentlicht wurden.
- Kaspersky Lab hat gemeinsam mit weiteren Mitgliedern des Industrial Internet Consortium (IIC) den „Security Maturity Model (SMM) Practioner's Guide“ (PDF) https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf entwickelt. Der Leitfaden unterstützt IoT-Betreiber bei der Einschätzung ihres aktuellen und anvisierten Security-Reifegrads. Zudem hilft der Guide bei der Optimierung des IoT-Sicherheitsniveaus und empfiehlt anhand von 36 Parametern entsprechende Verbesserungen

Basic-Level

So wichtig spezielle IT-Sicherheitslösungen für die besonderen Risiken im IoT und Industrial IoT auch sind, bereits bei dem Basisschutz, der in der klassischen IT üblich ist, könnte so manches verbessert werden, sofern die IoT-Lösungen entsprechende Einstellungen und Funktionen bieten:

- Passwortschutz aktivieren
- Standardeinstellungen ändern
- Keine Jailbreaks von Geräten oder Installationen von Anwendungen nicht verifizierter Marktplätze Dritter
- Geräte-Firmware aktualisieren
- Verschlüsselung sowohl in Festplatten als auch in Kommunikationsplattformen aktivieren
- Regelmässige Backups der Konfigurations- und Automatisierungsregeldateien des IoT-Automatisierungsservers erstellen

3.1.9 Schutz vor Profiling

Die Nutzer können vielfach direkt oder indirekt identifiziert werden, sei es z.B. durch die Gerätekennzeichnung oder eine Registrierung der Nutzer für ein bestimmtes Gerät. Die IoT-Daten können so zu Nutzerprofilen und zum sog. Tracking (deutsch: Verfolgung) führen. Oftmals werden so Standortdaten der Geräte und ihrer Nutzer erhoben, gespeichert und ausgewertet, die Rückschlüsse auf Personen und ihr Verhalten zulassen. IoT-Anbieter müssen hierfür eine entsprechende Rechtsgrundlage haben (z.B. eine Einwilligung der Nutzer).

3.2 Cloudcomputing

Cloud Computing hat in den letzten Jahren stetig zugenommen, auch wenn sich manche Versprechen der Anfangszeit nicht in dem Mass erfüllt haben, wie prognostiziert. Man kann jedenfalls nicht mehr von einem Hype sprechen, sondern Cloud Computing ist in vielen Bereichen bereits zum Standard avanciert.
Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden.

Basic-Level

Privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, will mit diesem Merkblatt aufzeigen, welche Risiken bei Cloud- und ähnlichen Dienstleistungen zusätzlich zu denen einer herkömmlichen Auftragsdatenbearbeitung hinzukommen oder sich akzentuieren und wie die Verantwortung diesbezüglich von den öffentlichen Organen konkret wahrgenommen werden kann.
Das Merkblatt legt den Fokus auf datenschutzrechtliche Risiken. Die öffentlichen Organe müssen andere Risiken für ihre Aufgabenerfüllung – z.B. bei der Durchsetzung von Vertragsbestimmungen oder bezüglich Datensouveränität – selbst mitberücksichtigen.
Der Leitfaden Nutzung externer Cloud-Dienste des Datenschutzbeauftragten des Kantons Zürich richtet sich an Mitarbeitende öffentlicher Organe, die Cloud-Dienste evaluieren. Er zeigt auf, welche Punkte bei der Nutzung externer Cloud-Dienste zu berücksichtigen sind und wie bei der Auswahl von Cloud-Diensten vorzugehen ist.
Die Vorgaben des Merkblattes bzw. des Leitfadens lassen sich auf den privatwirtschaftlichen Bereich übertragen.

3.3 Gesundheitsbereich

3.3.1 Bearbeiten von Gesundheitsdaten im medizinischen Bereich

Die rasche Entwicklung der Informations- und Kommunikationstechnik hat die Bearbeitung von Personendaten im Gesundheitswesen erheblich vereinfacht. Durch die elektronische Datenbearbeitung können Daten über die Gesundheit blitzschnell gespeichert, abgerufen und an Dritte weitergegeben werden. Gesundheitsdaten gehören zu den besonders schützenswerten Personendaten. Ein Missbrauch von solchen Daten kann gravierende Folgen für die betroffenen Personen haben.

Basic-Level

Wer schützenswerte Daten bearbeitet, muss entweder eine explizite Einwilligung der Betroffenen oder einen anderen Rechtfertigungsgrund nachweisen oder sich auf eine hinreichend bestimmte Grundlage im Gesetz berufen können. Dem hohen Schutzbedarf von Gesundheitsdaten muss bei deren Bearbeitung auch durch taugliche Sicherheitsvorkehren Rechnung getragen werden. Die Anforderungen an die technische Sicherheit werden durch die neue Datenschutzgesetzgebung verschärft.
Die Verordnung zum Datenschutzgesetz legt fest, dass Privatpersonen, die Personendaten bearbeiten, für die Vertraulichkeit dieser Daten sorgen müssen. Für patientenbezogene Daten kommen die strafrechtlich geschützten Berufsgeheimnisse der Medizinalpersonen hinzu. Diese verpflichten auch deren Hilfspersonen – und als solche gelten zum Beispiel auch Mitarbeitende von Cloud-Diensten, wenn sie Zugriff auf Gesundheitsdaten der Kunden haben.
Ob der Datenschutz und das Berufsgeheimnis rechtlich hinreichend geschützt, durchsetzbar und durch entsprechende Haftungsklauseln untermauert sind,

hängt von der Ausgestaltung der vertraglichen Vereinbarungen ab, die der Datenherr mit den Cloudanbietern abschliesst.

Befindet sich der Cloudstandort ausserhalb der Schweiz, kommt als zusätzliche Dimension hinzu, dass ausländische Behörden auf dort bearbeitete Daten zugreifen könnten. In Ländern mit einem Datenschutzniveau, das jenem der Schweiz gleichwertig ist – wie in den Staaten des Europäischen Wirtschaftsraums oder in Grossbritannien – erfolgen solche Zugriffe nur in einem justizförmigen Verfahren auf richterliche Anordnung hin. Beim Datenexport in andere Staaten muss hingegen damit gerechnet werden, dass die dortigen Behörden in intransparenter Weise auf die in einer Cloud bearbeiteten Daten zugreifen, ohne den Cloudbetreibern oder den direkt betroffenen Personen einen wirksamen Rechtschutz zu gewähren. Leider gehören nicht nur autoritäre, sondern auch demokratische Staaten wie die USA zum Kreis dieser Länder. Das macht den Export von Personendaten in Clouds, die auf US-Boden betrieben werden, kompliziert.
Gesundheitsdaten, die auf Datenträgern und Infrastrukturen des Arbeitgebers bearbeitet werden, dürfen weder auf private Datenträger wie ein Smartphone kopiert noch über privat benutzte Kanäle wie WhatsApp weitergegeben werden. Solches Tun sprengt den Rahmen der in den internen Nutzungsreglementen autorisierten Datenbearbeitungen und unterläuft die technischen Sicherheitsvorkehren, mit denen Unternehmen und Gesundheitseinrichtungen ihre Infrastrukturen schützen.

Expert-Level

3.3.2 Entwicklung von Gesundheits-Apps

Mit der Markteinführung des Smartphones hat sich in der Software-Entwicklung ein neues Entwicklungsfeld geöffnet. Apps zu diversen Themen sind gefragt und werden rege von Anwendern genutzt. Gerade Anwendungen zu medizinischen oder Lifestyle-Themen erscheinen zahlreich und mit einem sehr breiten Fokus. Im Rahmen von Gesundheits-Apps findet eine Bearbeitung von besonders schützenswerten Personendaten in Form von Gesundheitsdaten und je nach Sachlage auch von genetischen oder biometrischen Daten statt. Zudem findet die Bearbeitung verbreitet in Form von Profiling-Aktivitäten statt. Entsprechend gelten für die Bearbeitung von Personendaten im Bereich von Gesundheits-Apps aus datenschutzrechtlicher Sicht hohe bis sehr hohe Anforderungen.

3.3.3 Weitere Informationen

- Bearbeitung von Personendaten im medizinischen Bereich (admin.ch)
  Das Ziel dieses Leitfadens besteht darin, sowohl Patienten als auch Ärzte und weitere Medizinal-Personen auf die praktische Bedeutung der ärztlichen Schweigepflicht aufmerksam zu machen und für datenschutzrechtliche Aspekte (Schutz der Persönlichkeit der Betroffenen) zu sensibilisieren.
- Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer
  Praktische Hinweise: Umsetzungshilfe (e-health-suisse.ch)

4 Übungsaufgaben

Mögliche Lösungen zu den Übungsaufgaben befinden sind Kapitel 5.

4.1 Übungsaufgabe 1: Datenschutz- Analyse für die Fitness-Tracking-Anwendung

Angenommen, Sie arbeiten als Softwareentwickler in einem Unternehmen und sollen eine neue mobile Anwendung entwickeln, die es Benutzern ermöglicht, ihre täglichen Fitnessaktivitäten zu verfolgen. Die Anwendung soll personenbezogene Daten wie den Namen, das Geburtsdatum, das Geschlecht, die E-Mail-Adresse und die Gesundheitsdaten der Benutzer erfassen.

Erstellen Sie eine Analyse, um die Datenschutzanforderungen für diese Anwendung zu identifizieren.

4.2 Übungsaufgabe 2 Datenschutzanforderungen bei der Entwicklung digitaler Anwendungen

Angenommen, Sie arbeiten als Softwareentwickler in einem Unternehmen, das eine neue mobile App entwickelt. Diese App soll es den Benutzern ermöglichen, ihre persönlichen Gesundheitsdaten zu verwalten, einschliesslich Informationen zu ihren medizinischen Diagnosen, verschriebenen Medikamenten und Arztbesuchen. Ihre Aufgabe besteht darin, die Datenschutzanforderungen für diese App zu identifizieren und entsprechende Massnahmen zu empfehlen, um den Schutz der Benutzerdaten zu gewährleisten.

Teil 1: Identifizieren Sie die relevanten Datenschutzanforderungen für die mobile Gesundheits-App. Beschreiben Sie kurz, welche Art von Informationen geschützt werden müssen und warum.

Teil 2: Empfehlen Sie konkrete Massnahmen, die das Unternehmen ergreifen kann, um die Datenschutzanforderungen umzusetzen. Beschreiben Sie für jede Massnahme, wie sie zum Schutz der Benutzerdaten beiträgt.

4.3 Übungsaufgabe3 Datenschutz bei der Speicherung von Daten in der Cloud

Angenommen, Sie arbeiten als IT-Berater für ein Unternehmen, das beabsichtigt, seine sensiblen Kundendaten in der Cloud zu speichern. Ihre Aufgabe besteht darin, die Datenschutzanforderungen für die Speicherung solcher Daten in der Cloud zu identifizieren und entsprechende Massnahmen zur Sicherstellung des Datenschutzes vorzuschlagen.

Teil 1: Identifizieren Sie die relevanten Datenschutzanforderungen für die Speicherung sensibler Kundendaten in der Cloud. Beschreiben Sie kurz, warum diese Anforderungen wichtig sind.

Teil 2: Empfehlen Sie konkrete Massnahmen, die das Unternehmen ergreifen kann, um die Datenschutzanforderungen bei der Speicherung sensibler Kundendaten in der Cloud zu erfüllen. Beschreiben Sie für jede Massnahme, wie sie zum Schutz der Kundendaten beiträgt.

Es ist zu beachten, dass die konkreten Massnahmen je nach Cloud-Anbieter, den verwendeten Technologien und den geltenden Datenschutzbestimmungen variieren können.

4.4 Übungsaufgabe 4 Datenschutz und Cloud-Speicherung: Identifizierung geeigneter Daten für die Speicherung in der Cloud

Sie arbeiten als Datenschutzbeauftragter eines Unternehmens, das beabsichtigt, einen Teil seiner Daten in der Cloud zu speichern. Ihre Aufgabe besteht darin, zu analysieren, welche Art von Daten oder unter welchen Voraussetzungen bestimmte Daten in der Cloud gespeichert werden können. Begründen Sie Ihre Entscheidungen jeweils unter Berücksichtigung der Datenschutzanforderungen.

Teil 1: Identifizieren Sie drei Arten von Daten, die potenziell in der Cloud gespeichert werden könnten, und erläutern Sie, welche Voraussetzungen erfüllt sein sollten, um eine sichere und datenschutzkonforme Speicherung in der Cloud zu ermöglichen.

Teil 2: Nennen Sie drei Arten von Daten, die aus datenschutzrechtlichen Gründen nicht in der Cloud gespeichert werden sollten, und erläutern Sie, warum dies der Fall ist.

Um die in Teil 2 genannten Arten von Daten (personenbezogene Gesundheitsdaten, Finanzdaten und vertrauliche Kundeninformationen) dennoch in der Cloud speichern zu können, müssen bestimmte Massnahmen ergriffen werden, um den Datenschutz zu gewährleisten.

Es ist zu beachten, dass trotz dieser Massnahmen ein gewisses Restrisiko besteht. Daher sollten Unternehmen stets eine sorgfältige Risikoanalyse durchführen und abwägen, ob die Vorteile der Cloud-Speicherung die potenziellen Risiken überwiegen.

4.5 Übungsaufgabe 5 Datenschutz und Cloud-Speicherung in einer Jugend-Partizipations-App

Sie sind als Datenschutzbeauftragter eines Unternehmens beauftragt worden, eine Jugend-Partizipations-App zu entwickeln, die es Jugendlichen ermöglicht, sich politisch zu engagieren. Ihre Aufgabe besteht darin, zu analysieren, welche Daten in der Cloud gespeichert werden können und unter welchen Voraussetzungen dies datenschutzkonform möglich ist. Begründen Sie Ihre Entscheidungen jeweils unter Berücksichtigung der Datenschutzanforderungen und des Schutzes der Privatsphäre der Jugendlichen.

Teil 1: Identifizieren Sie drei Arten von Daten, die in der Cloud gespeichert werden könnten, um die Jugend-Partizipations-App zu unterstützen. Erklären Sie, unter welchen Voraussetzungen diese Daten in der Cloud gespeichert werden können.

Teil 2: Identifizieren Sie drei Arten von Daten, die aus Datenschutzgründen nicht in der Cloud gespeichert werden sollten, und erläutern Sie, warum dies der Fall ist.

Es ist wichtig zu beachten, dass die genannten Datenkategorien und Empfehlungen je nach den spezifischen Datenschutzgesetzen und Anforderungen der Jugend-Partizipations-App variieren können. Bei der Entwicklung der App sollten daher die geltenden

Datenschutzgesetze und -vorschriften sorgfältig berücksichtigt und gegebenenfalls professioneller rechtlicher Rat eingeholt werden.

4.6 Übungsaufgabe 5 Datenschutzprobleme und Cloud-Speicherung bei der Visualisierung von Campus-Gebäuden und Entwicklungsplänen

Sie sind als Datenschutzbeauftragter der Fachhochschule OST in Rapperswil-Jona beauftragt worden, die datenschutzrechtlichen Aspekte bei der Visualisierung von Campus-Gebäuden und Entwicklungsplänen zu analysieren. Ihre Aufgabe besteht darin, zu prüfen, ob es Datenschutzprobleme gibt und zu begründen, welche Daten unter welchen Voraussetzungen in der Cloud gespeichert werden können. Nehmen Sie dabei insbesondere Bezug auf die Zielgruppengerechtigkeit der Visualisierung und die Beteiligung der Öffentlichkeit.

Teil 1: Analysieren Sie mögliche Datenschutzprobleme im Zusammenhang mit der Visualisierung von Campus-Gebäuden und Entwicklungsplänen. Begründen Sie, welche Probleme auftreten könnten und welche datenschutzrechtlichen Grundsätze betroffen sein könnten.

Teil 2: Begründen Sie, welche Daten unter welchen Voraussetzungen in der Cloud gespeichert werden können, um eine datenschutzkonforme Visualisierung und Beteiligung zu ermöglichen.

Hinweis: Die konkrete Lösung der Aufgabe kann je nach den geltenden Datenschutzgesetzen und -richtlinien variieren. Es ist wichtig, die spezifischen rechtlichen Anforderungen und Datenschutzbestimmungen des betreffenden Landes zu berücksichtigen.

4.7 Übungsaufgabe 5 Datenschutzprobleme Demenz und Smart Home

Herr Mustermann ist an Demenz erkrankt. Er kann sich Informationen nicht mehr so gut merken und hat Schwierigkeiten, Gesprächen zu folgen oder verlegt Gegenstände. Einfache Alltagsaufgaben wie einkaufen, Wäsche trocknen oder Essen kochen kann er allein bewältigen, aber komplizierte Anforderungen (z.B. eine Banküberweisungen zu tätigen) schafft er nur mit Unterstützung.
Eines Tages verlässt er seine Wohnung zum Einkaufen. Die Oberlichter sind offen, weil er die kühle Abendluft nutzen möchte, um die Wohnung zu kühlen. Als er 30 Minuten Fussweg von seiner Wohnung entfernt ist, entsteht ein heftiges Sommergewitter. Herr Mustermann hat Sorge, dass ein Wetterschaden entsteht. Welche technischen Ansätze können Herrn Mustermann unterstützen?

Diese technischen Ansätze bieten verschiedene Möglichkeiten, um Herr Mustermann dabei zu unterstützen, seine Sorgen bezüglich der Wohnungsschäden zu mindern und seine Selbstständigkeit zu bewahren. Es ist jedoch wichtig, dass er sich bei der Auswahl und Implementierung solcher Technologien auch über Datenschutz- und Sicherheitsaspekte informiert und gegebenenfalls professionelle Beratung einholt.

Teil 1:

Angenommen, Sie sind ein Datenschutzexperte und wurden beauftragt, die technischen Lösungsmöglichkeiten für Herr Mustermann zu bewerten und sicherzustellen, dass der

Datenschutz gewährleistet ist. Ihre Aufgabe besteht darin, die Datenschutzaspekte der vorgeschlagenen technischen Lösungen zu analysieren und Empfehlungen zu geben.

Hinweis: Berücksichtigen Sie bei der Lösung dieser Aufgabe die rechtlichen Rahmenbedingungen und Datenschutzbestimmungen Ihres Landes. Zu Lösung gehören folgende Schritte

- Identifikation der technischen Lösungen
- Analyse der Datenschutzaspekte
- Bewertung der Datenschutzrisiken
- Empfehlungen und Massnahmen zur Minimierung der Risiken
- Schriftliche Bewertung

Hinweis: Die konkreten technischen Lösungen und Datenschutzmassnahmen können je nach Kontext und rechtlichen Bestimmungen variieren. Die oben genannten Lösungen dienen nur als Beispiel und sollten an die spezifischen Anforderungen und Vorschriften angepasst werden.

5 Lösungswege zu den Übungsaufgaben

5.1 Übungsaufgabe 1: Datenschutz- Analyse für die Fitness-Tracking-Anwendung

Angenommen, Sie arbeiten als Softwareentwickler in einem Unternehmen und sollen eine neue mobile Anwendung entwickeln, die es Benutzern ermöglicht, ihre täglichen Fitnessaktivitäten zu verfolgen. Die Anwendung soll personenbezogene Daten wie den Namen, das Geburtsdatum, das Geschlecht, die E-Mail-Adresse und die Gesundheitsdaten der Benutzer erfassen.

Erstellen Sie eine Analyse, um die Datenschutzanforderungen für diese Anwendung zu identifizieren.

Mögliche Lösung:

Datenschutz- Analyse für die Fitness-Tracking-Anwendung:

1. Schritt: Beschreibung der geplanten Datenverarbeitung

    - Erfassung sensibler personenbezogener Daten (Name, Geburtsdatum, Geschlecht, E-Mail-Adresse, Gesundheitsdaten)
    - Verarbeitung und Speicherung der Daten auf den Servern des Unternehmens
    - Zugriff auf die Daten durch autorisierte Mitarbeiter zur Fehlerbehebung und Support-Zwecke

2. Schritt: Bewertung der Notwendigkeit einer Analyse

    - Die Verarbeitung sensibler personenbezogener Daten erfordert eine genaue Überprüfung der Datenschutzrisiken.

- Die geplante Anwendung kann möglicherweise hohe Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringen.

3. Schritt: Beurteilung der Datenschutzrisiken

   a) Identifikation der Risiken:

   - Unbefugter Zugriff auf die gesammelten Daten durch Dritte
   - Datenverlust oder -beschädigung während der Übertragung oder Speicherung
   - Fehlende Sicherheitsmassnahmen zum Schutz der Daten
   - Mögliche Verwendung der Daten für unberechtigte Zwecke

   b) Bewertung der Risiken:

   - Hohe Risiken: Unbefugter Zugriff auf sensible personenbezogene Daten und mögliche Schäden für die Privatsphäre und den Datenschutz der Benutzer.

4. Schritt: Massnahmen zur Risikominderung

   - Implementierung von Sicherheitsmassnahmen wie Zugriffsbeschränkungen, Verschlüsselung und sichere Datenübertragung
   - Datenschutzrichtlinien und Nutzungsbedingungen, um die Benutzer über den Umgang mit ihren Daten zu informieren und ihre Zustimmung einzuholen
   - Regelmässige Sicherheitsüberprüfungen und Aktualisierungen der Anwendung, um potenzielle Schwachstellen zu identifizieren und zu beheben

5. Schritt: Dokumentation der Ergebnisse

   - Zusammenfassung der identifizierten Risiken und der ergriffenen Massnahmen zur Risikominderung
   - Verweis auf die Datenschutzrichtlinien und Nutzungsbedingungen

5.2 Übungsaufgabe 2 Datenschutzanforderungen bei der Entwicklung digitaler Anwendungen

Angenommen, Sie arbeiten als Softwareentwickler in einem Unternehmen, das eine neue mobile App entwickelt. Diese App soll es den Benutzern ermöglichen, ihre persönlichen Gesundheitsdaten zu verwalten, einschliesslich Informationen zu ihren medizinischen Diagnosen, verschriebenen Medikamenten und Arztbesuchen. Ihre Aufgabe besteht darin, die Datenschutzanforderungen für diese App zu identifizieren und entsprechende Massnahmen zu empfehlen, um den Schutz der Benutzerdaten zu gewährleisten.

Teil 1: Identifizieren Sie die relevanten Datenschutzanforderungen für die mobile Gesundheits-App. Beschreiben Sie kurz, welche Art von Informationen geschützt werden müssen und warum.

Mögliche Lösung:

Die relevanten Datenschutzanforderungen für die mobile Gesundheits-App sind wie folgt:

1. Schutz personenbezogener Daten: Da die App persönliche Gesundheitsdaten der Benutzer verarbeitet, müssen die Daten geschützt und vor unbefugtem Zugriff geschützt werden, um die Privatsphäre der Benutzer zu gewährleisten.
2. Einwilligung der Benutzer: Bevor die App personenbezogene Gesundheitsdaten sammelt oder verarbeitet, muss sie die ausdrückliche Einwilligung der Benutzer einholen. Die Benutzer sollten über den Zweck der Datenerhebung und die Art der Verarbeitung informiert werden.
3. Datensparsamkeit: Die App sollte nur die für ihre Funktionen unbedingt erforderlichen Daten sammeln und speichern. Es sollten keine überflüssigen oder unnötigen Daten erhoben werden.
4. Datenintegrität und -genauigkeit: Die App muss sicherstellen, dass die gesammelten Daten korrekt, vollständig und aktuell sind. Es sollten Mechanismen implementiert werden, um sicherzustellen, dass die Datenqualität aufrechterhalten wird.
5. Datensicherheit: Die App muss angemessene technische und organisatorische Massnahmen implementieren, um die Sicherheit der gesammelten Daten zu gewährleisten. Dazu gehören der Schutz vor unbefugtem Zugriff, Verschlüsselung sensibler Daten und regelmässige Sicherheitsüberprüfungen.

Teil 2: Empfehlen Sie konkrete Massnahmen, die das Unternehmen ergreifen kann, um die Datenschutzanforderungen umzusetzen. Beschreiben Sie für jede Massnahme, wie sie zum Schutz der Benutzerdaten beiträgt.

Mögliche Lösung:

1. Implementierung einer sicheren Datenübertragung: Die App sollte eine sichere Kommunikationsprotokolle wie HTTPS verwenden, um sicherzustellen, dass die übertragenen Daten verschlüsselt sind und vor Abhörversuchen geschützt werden.
2. Datenschutzrichtlinien und -erklärungen: Das Unternehmen sollte klare Datenschutzrichtlinien und -erklärungen bereitstellen, die den Benutzern erklären, welche Daten gesammelt werden, wie sie verwendet werden und welche Rechte die Benutzer in Bezug auf ihre Daten haben.
3. Zugriffskontrollen: Die App sollte Zugriffskontrollmechanismen implementieren, um sicherzustellen

5.3 Übungsaufgabe3 Datenschutz bei der Speicherung von Daten in der Cloud

Angenommen, Sie arbeiten als IT-Berater für ein Unternehmen, das beabsichtigt, seine sensiblen Kundendaten in der Cloud zu speichern. Ihre Aufgabe besteht darin, die Datenschutzanforderungen für die Speicherung solcher Daten in der Cloud zu identifizieren und entsprechende Massnahmen zur Sicherstellung des Datenschutzes vorzuschlagen.

Teil 1: Identifizieren Sie die relevanten Datenschutzanforderungen für die Speicherung sensibler Kundendaten in der Cloud. Beschreiben Sie kurz, warum diese Anforderungen wichtig sind.

Mögliche Lösung:

Die relevanten Datenschutzanforderungen für die Speicherung sensibler Kundendaten in der Cloud sind wie folgt:

1. Datensicherheit: Die sensiblen Kundendaten müssen vor unbefugtem Zugriff und Diebstahl geschützt werden. Es ist wichtig sicherzustellen, dass die Daten während der Übertragung und im Ruhezustand verschlüsselt sind, um die Vertraulichkeit der Daten zu gewährleisten.
2. Datenintegrität: Die gespeicherten Daten dürfen während der Übertragung oder Speicherung nicht unbemerkt verändert oder beschädigt werden. Es ist erforderlich, Mechanismen zu implementieren, um sicherzustellen, dass die Integrität der Daten gewahrt bleibt.
3. Datenschutz und Zugriffskontrolle: Es muss sichergestellt werden, dass nur autorisierte Personen auf die Kundendaten zugreifen können. Angemessene Zugriffskontrollen müssen implementiert werden, um sicherzustellen, dass die Daten nur für berechtigte Benutzer zugänglich sind.
4. Compliance mit Datenschutzgesetzen: Die Speicherung sensibler Kundendaten in der Cloud unterliegt möglicherweise spezifischen Datenschutzgesetzen. Es ist wichtig sicherzustellen, dass die Speicherung der Daten den gesetzlichen Anforderungen entspricht und die Zustimmung der Kunden eingeholt wurde.

Teil 2: Empfehlen Sie konkrete Massnahmen, die das Unternehmen ergreifen kann, um die Datenschutzanforderungen bei der Speicherung sensibler Kundendaten in der Cloud zu erfüllen. Beschreiben Sie für jede Massnahme, wie sie zum Schutz der Kundendaten beiträgt.

1. Mögliche Verschlüsselung der Daten: Alle sensiblen Kundendaten sollten vor der Übertragung zur Cloud und während der Speicherung verschlüsselt werden. Dies stellt sicher, dass selbst bei unbefugtem Zugriff auf die Daten keine verwertbaren Informationen abgerufen werden können.
2. Sichere Übertragung: Die Daten sollten über sichere Verbindungen übertragen werden, z. B. mittels HTTPS-Protokoll, um die Vertraulichkeit und Integrität der Daten während der Übertragung zu gewährleisten.
3. Zugriffskontrollen: Es sollten angemessene Zugriffskontrollen implementiert werden, um sicherzustellen, dass nur autorisierte Personen auf die Kundendaten zugreifen können. Dies kann durch die Verwendung von Benutzerkonten, Rollen und Berechtigungen erreicht werden.
4. Datensicherungsstrategie: Es sollte eine regelmässige Sicherung der gespeicherten Daten implementiert werden, um Datenverlust zu verhindern und die Wiederherstellbarkeit im Notfall sicherzustellen.
5. Vertragliche Vereinbarungen mit Cloud-Anbietern: Es ist wichtig, Verträge mit Cloud-Anbietern abzuschliessen, die die Einhaltung von Datenschutzbestimmungen und den Schutz der Kundendaten gewährleisten.

Es ist zu beachten, dass die konkreten Massnahmen je nach Cloud-Anbieter, den verwendeten Technologien und den geltenden Datenschutzbestimmungen variieren können.

5.4 Übungsaufgabe 4 Datenschutz und Cloud-Speicherung: Identifizierung geeigneter Daten für die Speicherung in der Cloud

Sie arbeiten als Datenschutzbeauftragter eines Unternehmens, das beabsichtigt, einen Teil seiner Daten in der Cloud zu speichern. Ihre Aufgabe besteht darin, zu analysieren, welche Art von Daten oder unter welchen Voraussetzungen bestimmte Daten in der Cloud gespeichert werden können. Begründen Sie Ihre Entscheidungen jeweils unter Berücksichtigung der Datenschutzanforderungen.

Teil 1: Identifizieren Sie drei Arten von Daten, die potenziell in der Cloud gespeichert werden könnten, und erläutern Sie, welche Voraussetzungen erfüllt sein sollten, um eine sichere und datenschutzkonforme Speicherung in der Cloud zu ermöglichen.

Mögliche Lösung:

1. Allgemeine Unternehmensdokumente: Dokumente wie Richtlinien, Präsentationen oder interne Mitteilungen können in der Cloud gespeichert werden, sofern sie keine personenbezogenen Daten enthalten und keinen sensiblen Informationen ausgesetzt sind. Es ist wichtig sicherzustellen, dass diese Dokumente keinerlei personenbezogene oder vertrauliche Informationen enthalten, um die Privatsphäre und Vertraulichkeit der Mitarbeiter und des Unternehmens zu schützen.

2. Anonymisierte Nutzungsstatistiken: Wenn das Unternehmen anonymisierte Nutzungsstatistiken von seinen digitalen Anwendungen sammelt, können diese in der Cloud gespeichert werden. Es ist wichtig sicherzustellen, dass die Daten ordnungsgemäss anonymisiert sind, so dass keine Rückschlüsse auf individuelle Benutzer möglich sind. Zusätzlich sollten geeignete Sicherheitsmassnahmen ergriffen werden, um die Integrität und Vertraulichkeit der Statistiken zu gewährleisten.
3. Nicht-personenbezogene Daten für Analysezwecke: Wenn das Unternehmen nicht-personenbezogene Daten für Analysezwecke sammelt, wie beispielsweise Verkaufsdaten oder demografische Informationen, können diese in der Cloud gespeichert werden. Es ist wichtig sicherzustellen, dass die Daten keine personenbezogenen Informationen enthalten und angemessene Sicherheitsmassnahmen implementiert werden, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

Teil 2: Nennen Sie drei Arten von Daten, die aus datenschutzrechtlichen Gründen nicht in der Cloud gespeichert werden sollten, und erläutern Sie, warum dies der Fall ist.

Mögliche Lösung:

1. Personenbezogene Gesundheitsdaten: Da personenbezogene Gesundheitsdaten besonders sensibel sind und speziellen Datenschutzanforderungen unterliegen, sollten sie aus datenschutzrechtlichen Gründen nicht in der Cloud gespeichert werden. Die Cloud-Umgebung kann möglicherweise nicht ausreichend abgesichert sein, um den Schutz dieser hochsensiblen Informationen zu gewährleisten.
2. Finanzdaten: Finanzdaten wie Bankkontodaten oder Kreditkarteninformationen sollten nicht in der Cloud gespeichert werden, da sie ein hohes Risiko für betrügerische Aktivitäten und Identitätsdiebstahl darstellen. Es ist wichtig, solche

sensiblen Finanzdaten auf sicheren internen Systemen oder unter strikter Einhaltung der PCI-DSS-Standards zu speichern.
3. Vertrauliche Kundeninformationen: Vertrauliche Kundeninformationen wie Passwörter, Sozialversicherungsnummern oder andere personenbezogene Daten sollten nicht in der Cloud gespeichert werden, um das Risiko eines unbefugten Zugriffs oder einer Verletzung der Privatsphäre zu minimieren. Diese Daten sollten intern auf sicheren Systemen gespeichert werden, die den erforderlichen Datenschutzstandards entsprechen.

Um die in Teil 2 genannten Arten von Daten (personenbezogene Gesundheitsdaten, Finanzdaten und vertrauliche Kundeninformationen) dennoch in der Cloud speichern zu können, müssen bestimmte Massnahmen ergriffen werden, um den Datenschutz zu gewährleisten. Hier sind einige Schritte, die unternommen werden könnten:

1. Verschlüsselung: Bevor die Daten in die Cloud hochgeladen werden, sollten sie vollständig verschlüsselt werden. Dadurch wird sichergestellt, dass selbst bei unbefugtem Zugriff auf die Daten diese nicht lesbar sind. Sowohl während der Übertragung als auch im Ruhezustand sollten starke Verschlüsselungsalgorithmen verwendet werden.
2. Daten-Pseudonymisierung: Bei personenbezogenen Daten kann eine Pseudonymisierung angewendet werden, um die Identifizierung von Personen zu erschweren. Dabei werden personenbezogene Informationen entfernt oder durch anonyme Identifikatoren ersetzt, während gleichzeitig ein Bezug zur ursprünglichen Person erhalten bleibt. Auf diese Weise wird das Risiko einer Verletzung der Privatsphäre reduziert.
3. Zugriffskontrollen und Berechtigungsmanagement: Es sollten strenge Zugriffskontrollen implementiert werden, um sicherzustellen, dass nur autorisierte Benutzer auf die Daten zugreifen können. Dies umfasst die Verwendung von mehrstufiger Authentifizierung, die Vergabe individueller Zugriffsrechte basierend auf den Rollen der Benutzer und die regelmässige Überprüfung und Aktualisierung der Berechtigungen.
4. Sichere Datenübertragung: Bei der Übertragung der Daten zwischen dem Unternehmen und der Cloud sollten sichere Kommunikationsprotokolle wie HTTPS verwendet werden. Dadurch wird sichergestellt, dass die Daten während der Übertragung vor unbefugtem Zugriff geschützt sind.
5. Auswahl eines vertrauenswürdigen Cloud-Anbieters: Es ist wichtig, einen Cloud-Anbieter auszuwählen, der hohe Sicherheitsstandards und Datenschutzrichtlinien einhält. Der Anbieter sollte transparente Informationen über seine Sicherheitsmassnahmen, Zertifizierungen und Datenschutzbestimmungen bereitstellen. Es kann auch hilfreich sein, Referenzen oder Empfehlungen anderer Unternehmen zu prüfen, die bereits Erfahrungen mit dem Anbieter haben.
6. Rechtliche Aspekte prüfen: Bei der Speicherung sensibler Daten in der Cloud müssen auch die geltenden Datenschutzgesetze berücksichtigt werden. Es ist wichtig sicherzustellen, dass die Cloud-Speicherung im Einklang mit den rechtlichen Anforderungen steht und gegebenenfalls die Zustimmung der betroffenen Personen eingeholt wurde.
7. Datenzugriffskontrolle: Es sollten strenge Zugriffskontrollen implementiert werden, um sicherzustellen, dass nur autorisierte Personen auf die sensiblen Daten in der

Cloud zugreifen können. Dies umfasst die Verwendung starker Authentifizierungsmethoden wie mehrstufiger Authentifizierung und die Implementierung von Rollen und Berechtigungen, um den Zugriff auf die Daten zu steuern und zu überwachen.

8. Auditing und Überwachung: Es ist wichtig, eine umfassende Überwachung der Zugriffe auf die Daten in der Cloud durchzuführen. Dies kann durch die Implementierung von Audit-Logs und Überwachungstools erreicht werden, um verdächtige Aktivitäten zu erkennen und entsprechend zu reagieren.

Es ist zu beachten, dass trotz dieser Massnahmen ein gewisses Restrisiko besteht. Daher sollten Unternehmen stets eine sorgfältige Risikoanalyse durchführen und abwägen, ob die Vorteile der Cloud-Speicherung die potenziellen Risiken überwiegen.

5.5 Übungsaufgabe 5 Datenschutz und Cloud-Speicherung in einer Jugend-Partizipations-App

Sie sind als Datenschutzbeauftragter eines Unternehmens beauftragt worden, eine Jugend-Partizipations-App zu entwickeln, die es Jugendlichen ermöglicht, sich politisch zu engagieren. Ihre Aufgabe besteht darin, zu analysieren, welche Daten in der Cloud gespeichert werden können und unter welchen Voraussetzungen dies datenschutzkonform möglich ist. Begründen Sie Ihre Entscheidungen jeweils unter Berücksichtigung der Datenschutzanforderungen und des Schutzes der Privatsphäre der Jugendlichen.

Teil 1: Identifizieren Sie drei Arten von Daten, die in der Cloud gespeichert werden könnten, um die Jugend-Partizipations-App zu unterstützen. Erklären Sie, unter welchen Voraussetzungen diese Daten in der Cloud gespeichert werden können.

Mögliche Lösung:

1. Benutzerprofile: Die App kann Benutzerprofile enthalten, die Informationen über die Interessen und politischen Ansichten der Jugendlichen erfassen. Diese Daten können in der Cloud gespeichert werden, wenn die Zustimmung der Nutzer eingeholt wurde und die Daten ausreichend anonymisiert sind, um eine individuelle Identifizierung zu verhindern. Es ist wichtig sicherzustellen, dass die Daten verschlüsselt und durch angemessene Zugriffskontrollen geschützt sind, um die Privatsphäre der Jugendlichen zu wahren.
2. Aktivitätsprotokolle: Die App kann Aktivitätsprotokolle enthalten, die die Aktionen und Beiträge der Jugendlichen im Rahmen der politischen Partizipation verfolgen. Diese Protokolle können in der Cloud gespeichert werden, um eine konsistente Erfassung und Analyse der Aktivitäten zu ermöglichen. Die Speicherung dieser Daten sollte jedoch auf das erforderliche Minimum beschränkt sein und es sollten Mechanismen implementiert werden, um die Identität der Jugendlichen zu schützen und unerwünschte Offenlegungen zu verhindern.
3. Umfrageergebnisse: Die App kann Umfragen oder Abstimmungen enthalten, bei denen die Jugendlichen ihre Meinungen zu bestimmten Themen äussern können. Die Ergebnisse dieser Umfragen können in der Cloud gespeichert werden, um eine aggregierte Analyse und Visualisierung der Daten zu ermöglichen. Es ist wichtig sicherzustellen, dass die Umfrageergebnisse nicht auf individuelle Benutzer

zurückführbar sind und dass die Daten sicher gespeichert und vor unbefugtem Zugriff geschützt sind.

Teil 2: Identifizieren Sie drei Arten von Daten, die aus Datenschutzgründen nicht in der Cloud gespeichert werden sollten, und erläutern Sie, warum dies der Fall ist.

Mögliche Lösung:

1. Sensible persönliche Informationen: Sensible persönliche Informationen wie Geburtsdaten, Adressen oder Sozialversicherungsnummern sollten aus Datenschutzgründen nicht in der Cloud gespeichert werden. Diese Informationen bergen ein hohes Risiko für den Missbrauch oder die Identitätsdiebstahl und sollten daher auf sicheren internen Systemen gespeichert werden, die den Datenschutzstandards entsprechen.
2. Vertrauliche Diskussionen: Vertrauliche Diskussionen zwischen den Jugendlichen oder private Nachrichten sollten nicht in der Cloud gespeichert werden, um die Vertraulichkeit und Privatsphäre der Nutzer zu wahren. Solche sensiblen Kommunikationen sollten besser über Ende-zu-Ende-verschlüsselte Kommunikationskanäle innerhalb der App abgewickelt werden.
3. Authentifizierungsdaten: Benutzeranmeldeinformationen wie Passwörter oder biometrische Daten sollten nicht in der Cloud gespeichert werden, um das Risiko eines unbefugten Zugriffs oder einer Kompromittierung der Konten zu minimieren. Stattdessen sollten bewährte Verfahren zur sicheren Speicherung und Verwaltung von Authentifizierungsdaten implementiert werden, wie beispielsweise die Verwendung von sicheren Hashing- und Verschlüsselungsalgorithmen auf den internen Systemen der App.

Es ist wichtig zu beachten, dass die genannten Datenkategorien und Empfehlungen je nach den spezifischen Datenschutzgesetzen und Anforderungen der Jugend-Partizipations-App variieren können. Bei der Entwicklung der App sollten daher die geltenden Datenschutzgesetze und -vorschriften sorgfältig berücksichtigt und gegebenenfalls professioneller rechtlicher Rat eingeholt werden.

5.6 Übungsaufgabe 5 Datenschutzprobleme und Cloud-Speicherung bei der Visualisierung von Campus-Gebäuden und Entwicklungsplänen

Sie sind als Datenschutzbeauftragter der Fachhochschule OST in Rapperswil-Jona beauftragt worden, die datenschutzrechtlichen Aspekte bei der Visualisierung von Campus-Gebäuden und Entwicklungsplänen zu analysieren. Ihre Aufgabe besteht darin, zu prüfen, ob es Datenschutzprobleme gibt und zu begründen, welche Daten unter welchen Voraussetzungen in der Cloud gespeichert werden können. Nehmen Sie dabei insbesondere Bezug auf die Zielgruppengerechtigkeit der Visualisierung und die Beteiligung der Öffentlichkeit.

Teil 1: Analysieren Sie mögliche Datenschutzprobleme im Zusammenhang mit der Visualisierung von Campus-Gebäuden und Entwicklungsplänen. Begründen Sie, welche Probleme auftreten könnten und welche datenschutzrechtlichen Grundsätze betroffen sein könnten.

Mögliche Lösung:

1. Persönliche Identifikation: Bei der Visualisierung von Campus-Gebäuden und Entwicklungsplänen besteht die Gefahr, dass personenbezogene Daten von Einzelpersonen offengelegt werden. Wenn beispielsweise Personen auf den Visualisierungen erkennbar sind, kann dies eine Verletzung des Rechts auf Privatsphäre darstellen. Um dies zu vermeiden, sollten personenbezogene Daten sorgfältig anonymisiert oder pixeliert werden.
2. Standortdaten: Bei der Visualisierung des Campus und seiner Umgebung können Standortdaten wie GPS-Koordinaten oder Adressen eine Rolle spielen. Es ist wichtig sicherzustellen, dass solche Standortdaten nicht ohne Zustimmung der Betroffenen verwendet oder veröffentlicht werden. Es sollte transparent gemacht werden, wie diese Daten erhoben und verwendet werden und welche Kontrollmöglichkeiten die Betroffenen haben.
3. Nutzerinteraktion: Wenn die Visualisierung der Campus-Gebäude und Entwicklungspläne interaktiv ist und eine Bürgerbeteiligung ermöglicht, können weitere Datenschutzprobleme auftreten. Es ist wichtig sicherzustellen, dass bei der Interaktion mit der Plattform keine personenbezogenen Daten unbefugt erfasst oder gespeichert werden. Die Einwilligung der Nutzer sollte eingeholt werden, bevor personenbezogene Daten erhoben oder verarbeitet werden.

Teil 2: Begründen Sie, welche Daten unter welchen Voraussetzungen in der Cloud gespeichert werden können, um eine datenschutzkonforme Visualisierung und Beteiligung zu ermöglichen.

Mögliche Lösung:

1. Anonymisierte Daten: Für eine datenschutzkonforme Visualisierung können anonymisierte Daten in der Cloud gespeichert werden. Personenbezogene Daten sollten vor der Speicherung so weit wie möglich anonymisiert oder pseudonymisiert werden, um die Privatsphäre der Betroffenen zu schützen.
2. Zustimmung der Betroffenen: Um bestimmte personenbezogene Daten in der Cloud zu speichern, ist die Zustimmung der Betroffenen erforderlich. Bevor personenbezogene Daten veröffentlicht oder verarbeitet werden, sollte eine klare Einwilligung eingeholt werden. Die Betroffenen sollten über den Zweck der Datenverarbeitung informiert und über ihre Rechte aufgeklärt werden.
3. Datenminimierung: Es ist wichtig, nur die für die Visualisierung und Beteiligung notwendigen Daten in der Cloud zu speichern. Die Speicherung von Daten sollte auf ein Minimum beschränkt werden, um das Datenschutzrisiko zu minimieren. Es sollte regelmässig überprüft werden, ob bestimmte Daten noch benötigt werden und gegebenenfalls gelöscht werden.

Hinweis: Die konkrete Lösung der Aufgabe kann je nach den geltenden Datenschutzgesetzen und -richtlinien variieren. Es ist wichtig, die spezifischen rechtlichen Anforderungen und Datenschutzbestimmungen des betreffenden Landes zu berücksichtigen.

5.7 Übungsaufgabe 5 Datenschutzprobleme Demenz und Smart Home

Herr Mustermann ist an Demenz erkrankt. Er kann sich Informationen nicht mehr so gut merken und hat Schwierigkeiten, Gesprächen zu folgen oder verlegt Gegenstände. Einfache Alltagsaufgaben wie einkaufen, Wäsche trocknen oder Essen kochen kann er allein

bewältigen, aber komplizierte Anforderungen (z.B. eine Banküberweisungen zu tätigen) schafft er nur mit Unterstützung.
Eines Tages verlässt er seine Wohnung zum Einkaufen. Die Oberlichter sind offen, weil er die kühle Abendluft nutzen möchte, um die Wohnung zu kühlen. Als er 30 Minuten Fussweg von seiner Wohnung entfernt ist, entsteht ein heftiges Sommergewitter. Herr Mustermann hat Sorge, dass ein Wetterschaden entsteht:

Herr Mustermann befürchtet, dass ihm die Fähigkeit, allein in seiner Wohnung leben zu können, aberkannt wird

Hier sind einige technische Ansätze, die Herr Mustermann bei der Bewältigung seiner Herausforderungen unterstützen könnten:

1. Smarte Sensoren und Geräte: Zum Beispiel könnten Feuchtigkeitssensoren eingesetzt werden, um bei starkem Regen das Schliessen der Fenster zu aktivieren. Temperatursensoren könnten dabei helfen, ein angenehmes Raumklima aufrechtzuerhalten.
2. Automatisierte Fensteröffner: Automatische Fensteröffner können an den Fenstern angebracht werden und über einen voreingestellten Mechanismus verfügen, der das Öffnen und Schliessen der Fenster basierend auf bestimmten Kriterien steuert.
3. Smarte Assistenzsysteme: Herr Mustermann könnte ein smartes Assistenzsystem wie Amazon Echo oder Google Home verwenden, um seine Wohnung zu überwachen und zu steuern.
4. Überwachungskameras und Alarmanlagen: Herr Mustermann könnte Überwachungskameras in seiner Wohnung installieren, um potenzielle Schäden oder Gefahren frühzeitig zu erkennen
5. Mobile Apps und Fernzugriff: Herr Mustermann könnte eine mobile App verwenden, um den Zustand seiner Wohnung zu überwachen und bestimmte Aktionen aus der Ferne durchzuführen.

Diese technischen Ansätze bieten verschiedene Möglichkeiten, um Herr Mustermann dabei zu unterstützen, seine Sorgen bezüglich der Wohnungsschäden zu mindern und seine Selbstständigkeit zu bewahren. Es ist jedoch wichtig, dass er sich bei der Auswahl und Implementierung solcher Technologien auch über Datenschutz- und Sicherheitsaspekte informiert und gegebenenfalls professionelle Beratung einholt.

Teil 1:

Angenommen, Sie sind ein Datenschutzexperte und wurden beauftragt, die technischen Lösungsmöglichkeiten für Herr Mustermann zu bewerten und sicherzustellen, dass der Datenschutz gewährleistet ist. Ihre Aufgabe besteht darin, die Datenschutzaspekte der vorgeschlagenen technischen Lösungen zu analysieren und Empfehlungen zu geben.

1. Analysieren Sie jede technische Lösung hinsichtlich der Datenschutzaspekte. Identifizieren Sie die personenbezogenen Daten, die von den Lösungen erfasst, gespeichert oder verarbeitet werden könnten. Achten Sie darauf, dass personenbezogene Daten Informationen sind, die Herr Mustermann direkt oder indirekt identifizieren können.

2. Bewerten Sie die Datenschutzrisiken im Zusammenhang mit jeder technischen Lösung. Berücksichtigen Sie dabei die Datenschutzprinzipien, wie Datensparsamkeit, Zweckbindung, Informationspflicht, Datensicherheit und die Rechte von Herr Mustermann. Identifizieren Sie potenzielle Risiken wie unbefugten Zugriff, unsichere Datenübertragung oder unzureichende Löschung von Daten.
3. Entwickeln Sie Empfehlungen und Massnahmen, um die Datenschutzrisiken zu minimieren oder zu beseitigen. Denken Sie dabei an technische, organisatorische oder rechtliche Massnahmen, die ergriffen werden können, um den Datenschutz zu gewährleisten. Berücksichtigen Sie dabei auch den Datenschutz durch Design und standardmässige Datenschutzeinstellungen.
4. Verfassen Sie eine schriftliche Bewertung, in der Sie die verschiedenen technischen Lösungen hinsichtlich ihrer Datenschutzaspekte analysieren und bewerten. Erläutern Sie Ihre Einschätzungen und geben Sie konkrete Empfehlungen, wie die Datenschutzanforderungen eingehalten werden können. Betonen Sie dabei die Bedeutung der Transparenz, Einwilligung und Information für Herr Mustermann.

Hinweis: Berücksichtigen Sie bei der Lösung dieser Aufgabe die rechtlichen Rahmenbedingungen und Datenschutzbestimmungen Ihres Landes.

Mögliche Lösung:

Identifikation der technischen Lösungen

- Entwicklung einer smarten Sensorlösung zur Überwachung der Raumtemperatur und Luftfeuchtigkeit in Ottos Wohnung, um automatisches Lüften zu ermöglichen.
- Implementierung eines automatisierten Fensteröffners, der basierend auf den gemessenen Werten der smarten Sensoren die Fenster öffnet und schliesst.
- Entwurf eines smarten Assistenzsystems, das Otto bei alltäglichen Aufgaben unterstützt und Erinnerungen für wichtige Termine und Aufgaben bereitstellt.
- Einrichtung von Überwachungskameras zur Sicherstellung der Sicherheit in der Wohnung und zur Erkennung von ungewöhnlichen Ereignissen.
- Entwicklung einer mobilen App, die Otto bei der räumlichen und zeitlichen Orientierung unterstützt und ihm hilft, seine Aufgaben und Termine im Blick zu behalten.

Analyse der Datenschutzaspekte

- Erfassung personenbezogener Daten: In allen Lösungen werden möglicherweise personenbezogene Daten wie Name, Adresse, Bewegungsdaten, Gesundheitsdaten und persönliche Vorlieben erfasst.
- Speicherung und Verarbeitung von Daten: Die erfassten Daten können in einer sicheren Cloud-Umgebung gespeichert und von den jeweiligen Systemen verarbeitet werden.
- Datensparsamkeit: Es sollte nur die für die jeweilige Lösung erforderlichen Daten erfasst und gespeichert werden.
- Informationspflicht: Otto sollte vorab über den Zweck der Datenerfassung und -verarbeitung informiert werden.
- Datensicherheit: Es ist wichtig, angemessene Sicherheitsmassnahmen zu implementieren, um die Daten vor unbefugtem Zugriff zu schützen.

Bewertung der Datenschutzrisiken

- Potenzielle Risiken: Unbefugter Zugriff auf die gespeicherten Daten, unsichere Datenübertragung, Missbrauch der Kamerasysteme oder Verstoss gegen die Datenschutzbestimmungen.
- Bewertung: Die Datenschutzrisiken sollten als moderat bis hoch bewertet werden, da personenbezogene Daten erfasst und verarbeitet werden.

: Empfehlungen und Massnahmen zur Minimierung der Risiken

- Anonymisierung und Pseudonymisierung der erfassten Daten, um die Identifizierung von Otto zu erschweren.
- Implementierung einer starken Zugriffskontrolle und Verschlüsselungstechniken, um die Datensicherheit zu gewährleisten.
- Einholung der informierten Einwilligung von Otto für die Datenerfassung und -verarbeitung.
- Regelmässige Überprüfung der Sicherheitsmassnahmen und Aktualisierung gemäss den geltenden Datenschutzbestimmungen.

: Schriftliche Bewertung

- Eine schriftliche Bewertung sollte alle analysierten technischen Lösungen, die identifizierten Datenschutzrisiken sowie die empfohlenen Massnahmen zur Minimierung der Risiken umfassen.
- Es sollte betont werden, dass der Schutz der Privatsphäre und der Datenschutz von Otto von grösster Bedeutung sind und dass die Lösungen den geltenden Datenschutzbestimmungen entsprechen müssen.
- Es ist wichtig, auf die Wichtigkeit der Transparenz, Einwilligung und Information hinzuweisen und Otto in den Entscheidungsprozess einzubeziehen.

Hinweis: Die konkreten technischen Lösungen und Datenschutzmassnahmen können je nach Kontext und rechtlichen Bestimmungen variieren. Die oben genannten Lösungen dienen nur als Beispiel und sollten an die spezifischen Anforderungen und Vorschriften angepasst werden.