Stiftung Medienpädagogik Bayern

Viele Daten, viel Verantwortung!

Datenschutzrechtliche Grundlagen verstehen und im Arbeitsalltag anwenden

Medienführerschein
Werkstatt
Berufliche Schulen

Einführung

Willkommen in der Medienführerschein Werkstatt!

Die Medienführerschein Werkstatt für die beruflichen Schulen bietet Ihnen Unterrichtsmaterialien zum Thema Datenschutz. Für Unternehmen und Mitarbeiter-:innen ergeben sich aus den datenschutzrechtlichen Vorgaben Pflichten. Werden diese Pflichten missachtet, kann dies zum Teil rechtliche Folgen haben. Auszubildende gehen in ihrem beruflichen Alltag in der Regel auch häufig mit personenbezogenen Daten um. Aus diesem Grund ist es wichtig, dass sich die Schüler:innen mit dem Thema Datenschutz auseinandersetzen. In der Unterrichtseinheit thematisieren sie, welche Daten in ihrem Berufsalltag schutzwürdig sind, wie datenschutzrechtlich sensible Daten im Berufsalltag behandelt werden müssen und wieso Datenschutz in der heutigen Zeit eine so hohe Bedeutung hat. Ziel der Unterrichtseinheit ist es, die Schüler:innen für die Bedeutung des Datenschutzes zu sensibilisieren und sie auf datenschutzrechtlich relevante Situationen im Arbeitsalltag vorzubereiten.

In der Medienführerschein Werkstatt finden Sie einen fertigen Kurs. Er bietet einen Vorschlag für eine 90-minütige Unterrichtsstunde und ist konzipiert als Blended-Learning-Angebot, bei dem Online- und Offline-Lernphasen kombiniert werden.
Alle Inhalte des fertigen Kurses sind an den bayerischen Lehrplan angepasst und vom Staatsinstitut für Schulqualität und Bildungsforschung (ISB) geprüft.

Zur Dokumentation der Teilnahme können die Schüler:innen eine Urkunde erhalten. Die Urkunden können im Klassensatz unter www.medienfuehrerschein.bayern kostenlos bestellt werden.

Neben einem fertigen Kurs enthält die Medienführerschein Werkstatt auch Arbeits-materialien zur Erstellung eines eigenen mebis-Kurses für Ihren Unterricht und verschiedene Hintergrundtexte.

Die Medienführerschein Werkstatt ist ein Angebot der Stiftung Medienpädagogik Bayern. Mithilfe einer Förderung durch das Bayerische Staatsministerium für Unterricht und Kultus wurde das Angebot in den Jahren 2021/2022 weiter ausgebaut. Weitere Informationen zum Medienführerschein Bayern finden Sie unter www.medienfuehrerschein.bayern.

Wir freuen uns, dass Sie unser Angebot nutzen und wünschen Ihnen gutes Gelingen.

Ihre Stiftung Medienpädagogik Bayern

Lehrplanbezug & Kompetenzen

Bezüge zum Kompetenzrahmen für Medienbildung an bayerischen Schulen

Kompetenzbereich	Teilkompetenzen
1. Basiskompetenzen	1.1
2. Suchen und Verarbeiten	2.3, 2.4
3. Kommunizieren und Kooperieren	3.4
4. Produzieren und Präsentieren	4.4
5. Analysieren und Reflektieren	5.1, 5.3, 5.4

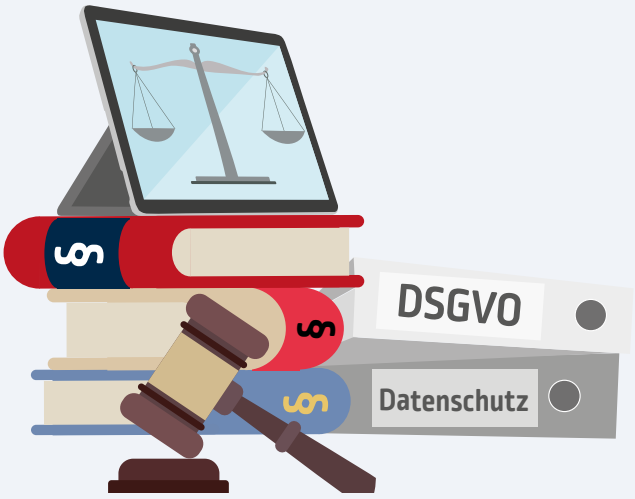
Bezüge zum LehrplanPLUS

Jgst.	Fach	Lernbereich
10	Deutsch (Regellehrplan für Berufsschule und Berufsfachschule)	Lesen – mit Texten und Medien umgehen – Handlungsphase: reflektieren
	Digitale Medien (Wahlpflichtlehrplan)	Umgang und Kommunikation mit digitalen Medien
	Ethik (Wahlmodul)	Lernbereich 10.2.1: Technikethik
11	Deutsch (Regellehrplan für Berufsschule und Berufsfachschule)	Schreiben – Handlungsphase: durchführen
	Digitale Medien (Wahlpflichtlehrplan)	Umgang und Kommunikation mit digitalen Medien
	Evangelische Religion	Lernbereich 2: Leben in Beziehung – Interaktion und Kommunikation
12	Digitale Medien (Wahlpflichtlehrplan)	Umgang und Kommunikation mit digitalen Medien
	Ethik (Wahlmodul)	Lernbereich 12.2.2: Digitale Ethik

Material & Vorbereitung

Werkstatt-Prinzip	In der Medienführerschein Werkstatt geht es zum einem darum, dass Lehrkräfte selbst aktiv werden und im besten Fall selbst etwas bauen. Und zwar medienpädagogische Online-Lern-Kurse für ihre Klassen. Dafür stehen im Werkstattbereich vorgefertigte Materialbausteine wie Film-Clips, interaktive Aufgaben oder Arbeitsblätter zur Verfügung. In der Medienführerschein Werkstatt findet sich zudem der fertige Kurs.
Fertiger Kurs	Der fertige Kurs bietet einen Vorschlag für eine 90-minütige Unterrichtseinheit. Er ist konzipiert als Blended-Learning-Angebot. Dabei werden Online- und Offline-Lernphasen kombiniert und z.B. die Ergebnisse der Online-Lernphasen gemeinsam in der Klasse reflektiert. **Hinweis:** Nutzen Sie für die Durchführung der Unterrichtseinheit auch die methodisch-didaktischen Informationen und Hintergrundinformationen. Diese finden Sie jeweils bei den zugehörigen Aufgabenstellungen.
Online-Lernplattform mebis	Informieren Sie sich im Vorfeld über mebis und ob es in Ihrer Schule Zugänge gibt. Weitere Hilfen stehen Ihnen unter mebis.bycs.de/kategorien/support-bereich zur Verfügung. Prüfen Sie auch den fertigen Kurs, da es optionale Angebote gibt, bei denen eine Vorauswahl getroffen werden muss.
Material	● **Für Lehrkräfte (blau):** Film-Clip: Die Azubis - Viele Daten, viel Verantwortung! Anleitung: Sortierübung Datensalat Tafelbild: Personenbezogene Daten Anleitung: H5P-Tool Question Set: Wichtige Begriffe des Datenschutzes Anleitung: H5P-Tool Dialog Cards: Wichtige Begriffe des Datenschutzes Anleitung: Digitales Element: Datenschutz-Parcours Auswertung: Digitales Element: Datenschutz-Parcours Tafelbild: Datenschutz im Unternehmensalltag Anleitung: H5P-Tool Check the Paragraphs: Goldene Regeln des Datenschutzes Tafelbild: Goldene Regeln des Datenschutzes ● **Für Schüler:innen (violett):** Film-Clip: Die Azubis - Viele Daten, viel Verantwortung! LearningApps.org: Sortierübung Datensalat H5P-Tool Question-Set: Wichtige Begriffe des Datenschutzes H5P-Tool Dialog Cards: Wichtige Begriffe des Datenschutzes Digitales Element: Datenschutz-Parcours H5P-Tool Check the Paragraphs: Goldene Regeln des Datenschutzes Merkblatt: Goldene Regeln des Datenschutzes

Empfohlene Hintergrund-texte	Information: Grundlagen des Datenschutzes Information: Bedeutung des Datenschutzes Information: Pflichten von Unternehmen Information: Pflichten von Arbeitnehmer:innen
Vorbereitung	Stellen Sie den Schüler:innen für die Durchführung des fertigen Kurses PCs, Laptops oder Tablets zur Verfügung. Aus Sicherheits- und Kompatibilitätsgründen ist die Verwendung eines aktuellen Betriebssystems und einer aktuellen Browserversion empfehlenswert. Vorab empfehlen wir außerdem einen Funktionstest von Geräten und Internetverbindung.



Ablauf des Unterrichts

Phase 1: Sensibilisierung & Wissenserarbeitung Datenschutz

	Für einen motivierenden Einstieg in das Thema steht der »Film-Clip: Die Azubis - Viele Daten, viel Verantwortung« (Dauer: 01:50 Min.) zur Verfügung. Der Film-Clip ist auch als Download verfügbar in der mebis Mediathek oder auf der Medienführerschein Website. Wählen Sie zwischen Plenum und Einzelarbeit aus: » 1.1 Option Plenum » 1.1 Option Einzelarbeit **Material:** Für Option Plenum benötigen Sie einen PC und einen Beamer. Für Option Einzelarbeit benötigt jede:r Schüler:in ein Endgerät (PC/Laptop/Tablet) und Kopfhörer. Verbergen Sie die nicht gewählte Option.		Film-Clip
1.1	Option: Plenum Schauen Sie den Film-Clip im Plenum an. Besprechen Sie im Anschluss kurz den Film-Clip. Fragen Sie, ob jemand in der Klasse ähnliche Situationen in Ausbildungsbetrieben erlebt hat.	**10'**	Film-Clip
	Option: Einzelarbeit Die Schüler:innen schauen sich den Film-Clip einzeln über ihr Endgerät (PC/Laptop/Tablet) an. Anschließend bearbeiten sie Multiple-Choice-Fragen zum Film-Clip. Fragen Sie im Anschluss, ob jemand in der Klasse ähnliche Situationen in Ausbildungsbetrieben erlebt hat.	**10'**	Film-Clip
1.2	Einzelarbeit: Datensalat Die Schüler:innen absolvieren in Einzelarbeit die »Sortierübung: Datensalat«. Sie ordnen 18 unterschiedliche Datenbeispiele den drei Kategorien zu: (1) personenbezogene Daten, (2) Geschäfts- und Betriebsgeheimnisse sowie (3) unproblematische Informationen. Besprechen Sie im Anschluss die richtigen Antworten gemeinsam im Plenum.	**05'**	Anleitung: Sortierübung LearningApps.org: Sortierübung Datensalat

1.3	Plenum: Personenbezogene Daten Erläutern Sie kurz, warum Datenschutz in der heutigen Zeit von großer Bedeutung ist. Im Anschluss erstellen Sie gemeinsam mit der Klasse das »Tafelbild: Personenbezogene Daten«, in dem Beispiele personenbezogener Daten fünf unterschiedlichen Gesprächssituationen zugeordnet werden. Das Tafelbild dient dazu, den Schüler:innen den Umgang mit personenbezogenen Daten in konkreten Gesprächssituationen vor Augen zu führen.	**10'**	Tafelbild: Personen-bezogene Daten
1.4	Plenum: Wichtige Begriff des Datenschutzes Die Schüler:innen lernen nun wichtige Begriffe des Datenschutzes und datenschutzrechtliche Vorgaben kennen. Wählen Sie zwischen zwei Optionen aus: » Option 1 H5P-Tool: Question-Set » Option 2 H5P-Tool: Dialog Cards Entscheiden Sie sich im Vorfeld der Unterrichtsstunde, welche Option Sie für Ihre Klasse nutzen möchten, und verbergen Sie die nicht gewählte Option.	**10'**	
	Option 1 H5P-Tool: Question-Set Die Schüler:innen beantworten in Einzelarbeit sechs Multiple-Choice-Fragen. **Option 2 H5P-Tool: Dialog Cards** Die Schüler:innen absolvieren die Übung in Einzelarbeit. Insgesamt werden fünf Begriffe erläutert. Bitten Sie die Schüler:innen, sich für jeden Begriff ein Beispiel zu überlegen und dieses auf einem Notizzettel für sich zu beantworten. **Hinweis:** Sie können auch nach jeder Frage bzw. Impulsfrage eine kurze Pause machen, um den jeweiligen Begriff gemeinsam zu besprechen.	**10'**	Anleitung: H5P-Tool: Question-Set H5P-Tool: Question-Set Anleitung: H5P-Tool: Dialog Cards H5P-Tool: Dialog Cards
1.5	Plenum: Reflexion Besprechen Sie die Begriffe zum Datenschutz, die die Schüler:innen in der Phase zuvor erarbeitet haben. Geben Sie ggf. ergänzende Erläuterungen zu den behandelten Grundbegriffen und gehen Sie auf Nachfragen der Schüler:innen ein. Sollten Sie in Phase 1.4 nach jedem Begriff eine kurze Besprechung im Plenum gemacht haben, können Sie die Reflexion dementsprechend verkürzen.	**10'**	

Phase 2: Datenschutz-Parcours

Die Schüler:innen kommen in ihrem Beruf täglich mit unterschiedlichen Daten in Kontakt und müssen die datenschutzrechtlichen Vorgaben kennen und anwenden können. Durch das Erleben von unterschiedlichen datenschutzrelevanten Situationen in einem digitalen Spiel sollen die Schüler:innen das Thema Datenschutz reflektieren und für einen verantwortungsvollen Umgang mit Daten sensibilisiert werden.

2.1 Einzelarbeit: Digitales Element: Datenschutz-Parcours

15‘

Anleitung: Digitales Element

Digitales Element

Auswertung: Digitales Element

Die Schüler:innen absolvieren in Einzelarbeit das »Digitale Element: Datenschutz-Parcours«. Hierfür benötigen sie ein Endgerät (PC/Laptop/Tablet) und Kopfhörer. Sie befinden sich in dem digitalen Element auf einem Raumschiff und werden mit acht Situationen konfrontiert, in denen sie den richtigen Umgang mit personenbezogen Daten angeben sollen. Im Anschluss erhalten die Schüler:innen ein PDF, in dem die persönliche Auswahl mit Feedback aufgelistet ist. Bitten Sie die Schüler:innen, die Ergebnisse des digitalen Elements in mebis hochzuladen.

2.2 Plenum: Reflexion

10‘

Anleitung: Digitales Element

Tafelbild: Datenschutz im Unternehmensalltag

Besprechen Sie mit den Schüler:innen die Ergebnisse des digitalen Elements. Fragen Sie zunächst, wie es den Schüler:innen gefallen hat. Stellen Sie im Anschluss einige Impulsfragen, z.B. „Haben Sie Situationen aus Ihrem eigenen Ausbildungsbetrieb wiedererkannt?“, „Gab es Beispiele, bei denen Ihnen die Einschätzung besonders schwerfiel?“. Im Anschluss erarbeiten Sie gemeinsam das »Tafelbild: Datenschutz im Unternehmensalltag«. Lassen Sie die Schüler:innen von persönlichen Erlebnissen in ihrem Arbeitsalltag berichten, die den im digitalen Element gezeigten Situationen ähneln. Motivieren Sie die Schüler:innen ihr eigenes Handeln zu hinterfragen.

Phase 3: Regeln

Die Schüler:innen haben nun das Basiswissen zum Thema „Personenbezogene Daten“. Im Folgenden sollen nun Regeln für den eigenen Berufsalltag entwickelt werden, an denen sich die Schüler:innen in der Praxis orientieren können.

3.1	Einzelarbeit: Regeln Die Schüler:innen absolvieren das »H5P-Tool: Check the Paragraphs«. Dabei überprüfen sie, ob die Formulierungen der einzelnen Datenschutzregeln richtig oder falsch sind. Durch das aufmerksame Durchlesen der einzelnen Satzteile prägen sich die Schüler:innen die allgemeinen Regeln des Datenschutzes ein.	**10‘**	Anleitung: H5P-Tool: Check the Paragraphs H5P-Tool: Check the Paragraphs
3.2	Plenum: Reflexion Gehen Sie im Tafelbild noch einmal gemeinsam mit der Klasse auf jede Regel ein. Lassen Sie die Schüler:innen ggf. zusätzlich eigene Regeln aufstellen und übertragen Sie das Gesagte in das Tafelbild. Lassen Sie die Schüler:innen über mögliche Konsequenzen diskutieren, die sich aus der Nichtbeachtung von Datenschutzregeln ergeben könnten und geben Sie Hinweise auf tatsächliche (berufliche und strafrechtliche) Konsequenzen bei Datenschutzverletzungen.	**15‘**	Tafelbild: Goldene Regeln des Datenschutzes
Optional erhalten die Schüler:innen am Ende der Unterrichtsstunde zur Dokumentation des Gelernten ein Merkblatt.			Merkblatt: Goldene Regeln des Datenschutzes

Anleitung:
Sortierübung: Datensalat

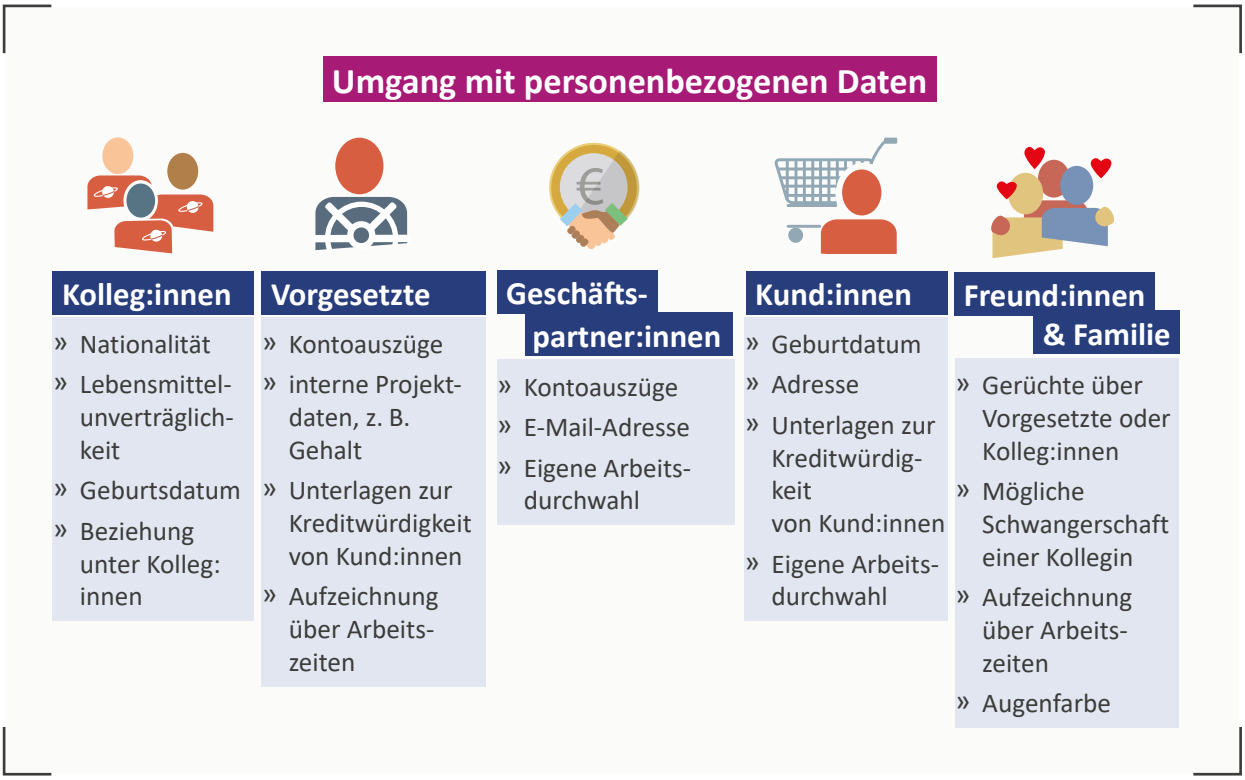
Aufgabe

Die Schüler:innen ordnen Beispiele für Daten den drei verschiedenen Kategorien zu, indem sie die Begriffe auf das richtige Feld ziehen (Drag&Drop-Prinzip). Bei der Zuordnung müssen sie entscheiden, ob es sich um unproblematische Informationen handelt, oder um sensiblen Daten, die geschützt werden müssen (Geschäfts- und Betriebsgeheimnissen sowie personenbezogenen Daten).

Geschäfts- und Betriebsgeheimnisse	» nicht veröffentlichte Umsatzzahlen » interne Projektdaten » Unterlagen zur Kreditwürdigkeit eines Unternehmens » Vertragsunterlagen zwischen verschiedenen Unternehmen » Konstruktionszeichnung
Personenbezogene Daten	» Geburtsdatum » Autokennzeichen eines privaten Fahrzeugs » Rentenversicherungsnummer » Nationalität » Unterlagen zur Kreditwürdigkeit von Kund:innen » Augenfarbe » Aufzeichnungen über Arbeitszeiten » E-Mail-Adresse » Aussage über Schwangerschaft einer Mitarbeiterin

Unproblematische Informationen	» Unternehmensanschrift » Kantinenpreise » Datum der Betriebsfeier » Anzahl der Mitarbeiter:innen

Tafelbild: Personenbezogene Daten



Einstieg

Erläutern Sie kurz, warum der Schutz personenbezogener Daten in der heutigen Zeit eine so große Bedeutung hat. Erfragen Sie, wo die Schüler:innen im eigenen Arbeitsalltag mit welchen personenbezogenen Daten in Berührung kommen.

Aufgabe

Lassen Sie die Schüler:innen Beispiele für personenbezogene Daten nennen (eine Wiederholung der Begriffe aus der vorherigen Aufgabe „Datensalat“ oder eigene Beispiele). Schreiben Sie diese Beispiele in die leeren Textfelder. Lassen Sie jedes Beispiel von der Klasse einer Spalte zuordnen.

» Darüber spreche ich mit meinen Kolleg:innen
» Darüber spreche ich mit meinen Vorgesetzten
» Darüber spreche ich mit den Geschäftspartner:innen
» Darüber spreche ich mit Kund:innen
» Darüber spreche ich mit Freund:innen und Familie

Beachten Sie, dass Situationen ggf. auch doppelt aufgelistet werden können. Machen Sie deutlich, dass es teilweise auch sehr subjektiv ist, was ich beispielsweise mit Kolleg:innen teile oder nicht (siehe Pläne für das Wochenende).

Persönliche Erfahrungen

Ermuntern Sie die Schüler:innen, von ihren persönlichen Erfahrungen zu erzählen. Die Schüler:innen achten auf die Beobachtungen ihrer Mitschüler:innen und vergleichen deren Erfahrungen im Umgang mit personenbezogenen Daten mit ihren eigenen Erfahrungen. Ziel ist es Aspekte auf das eigene Arbeitsumfeld zu übertragen.

Weitere Vorlagen

Sie können das Tafelbild im Gespräch mit den Schüler:innen an der Tafel entwickeln oder die mebis-Tafel bzw. PowerPoint-Vorlage nutzen.

Anleitung: H5P-Question-Set: Wichtige Begriffe des Datenschutzes

Diese Übung ist eine Alternative zum H5P-Tool Dialog Cards: Wichtige Begriffe des Datenschutzes. Wählen Sie nur eine der beiden Optionen aus.

Option

Die Schüler:innen absolvieren die Übung in Einzelarbeit. Das Quiz hat insgesamt sechs Fragen. Es ist ein Multiple-Choice-Quiz, d.h. es kann mehr als eine Antwort richtig sein.

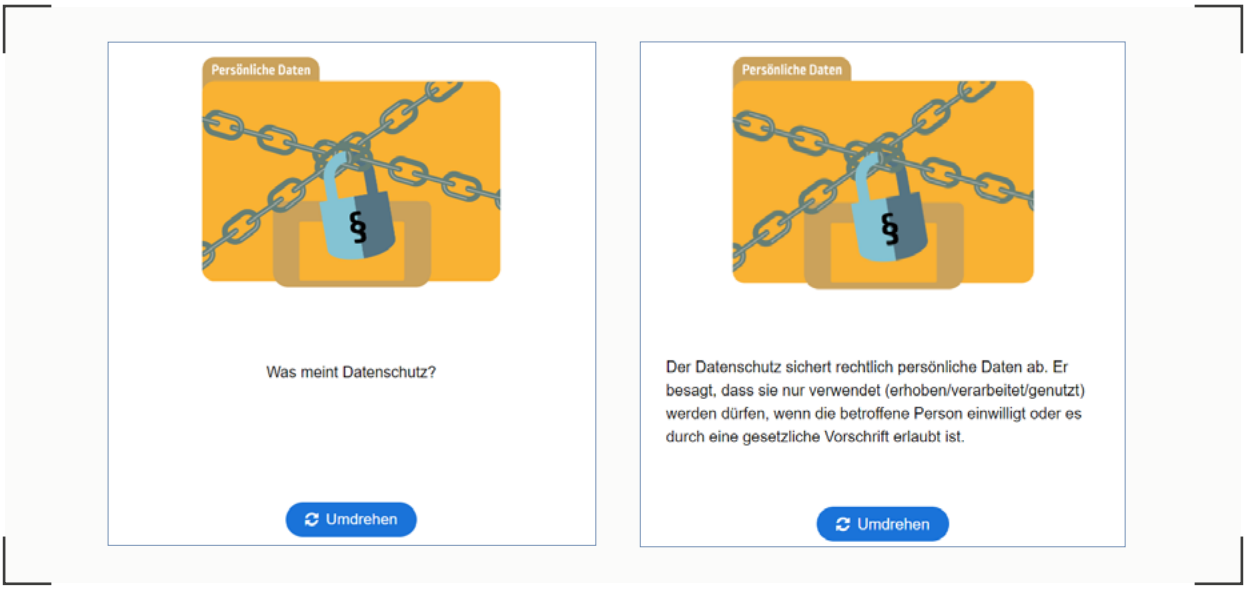
Aufgabe

Hinweis: Grüner Punkt 🟢 bedeutet: richtig, Roter Punkt 🔴 bedeutet: falsch.

1. Frage	**Sind persönliche Daten rechtlich geschützt?** 🟢 Ja 🔴 Nein 🔴 Nur von Personen ab 18 Jahren
2. Frage	**Persönliche Daten dürfen nur verwendet (erhoben/verarbeitet/genutzt) werden, wenn…?** 🟢 … der:die Betroffene einwilligt 🟢 … es durch eine gesetzliche Vorschrift erlaubt ist 🔴 … es gemeinnützigen Zwecken dient
3. Frage	**Was sind personenbezogene Daten?** 🟢 Daten, die einer konkreten Person zugeordnet werden können, z.B. Name, Geburtsdatum, Telefonnummer 🔴 Daten, die nur eine einzige Person wissen kann 🟢 Daten, die Rückschlüsse auf die Persönlichkeit erlauben
4. Frage	**Wann ist eine Person informationell selbstbestimmt?** 🟢 Wenn sie selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten bestimmen kann 🔴 Wenn sie selbstständig Informationen über Andere einholt 🔴 Wenn sie selbst bestimmt, welche Informationen Andere erhalten dürfen

5. Frage	**Welche Regeln gelten für eine (datenschutzrechtliche) Einwilligung?** ● Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn dies gesetzlich erlaubt ist oder die betroffene Person eingewilligt hat ● Eine Einwilligungserklärung kann standardisiert sein, sie muss allerdings freiwillig abgegeben werden ● Die betroffene Person ist über den Zweck der Datenerhebung, -verarbeitung und -nutzung, eine geplante Weitergabe der Daten an andere Unternehmen, die Möglichkeit nicht einwilligen zu müssen und die jederzeitige Widerrufsoption zu informieren
6. Frage	**Was ist Datensicherheit?** ● technische oder organisatorische Maßnahmen zum Schutz persönlicher Daten vor Diebstahl, Verfälschung, Missbrauch oder Beschädigung ● Zugang zu persönlichen Daten ausschließlich für autorisierte Personen ● Firewalls, Anti-Viren-Programme, Backup-Software, Verschlüsselungsprogramme

Anleitung: H5P-Tool Dialog Cards: Wichtige Begriffe des Datenschutzes



Option

Diese Übung ist eine Alternative zum H5P-Tool Question-Set: Wichtige Begriffe des Datenschutzes. Wählen Sie nur eine der beiden Optionen aus.

Aufgabe

Die Schüler:innen absolvieren die Übung in Einzelarbeit. Sie lesen jeweils eine Frage zu wichtigen Begriffen des Datenschutzes. Beim Anklicken der Karten erscheint die Rückseite mit einer Erläuterung. Bitten Sie die Schüler:innen, sich für jeden Begriff ein Beispiel zu überlegen und diese auf einem Notizzettel für sich zu beantworten. So lernen sie wichtige Begriffe des Datenschutzes und datenschutzrechtliche Vorgaben kennen.

Hinweis

Hinweis: Sie können auch nach jeder Frage eine kurze Pause machen, um den jeweiligen Begriff gemeinsam zu erarbeiten bzw. zu besprechen.

1. Dialogkarte: Datenschutz

Vorderseite:	**Rückseite:**
Was meint Datenschutz?	Der Datenschutz sichert rechtlich persönliche Daten ab. Er besagt, dass sie nur verwendet (erhoben/verarbeitet/genutzt) werden dürfen, wenn die betroffene Person einwilligt oder es durch eine gesetzliche Vorschrift erlaubt ist. **Hinweis für das Unterrichtsgespräch:** Regelungen sollen sicherstellen, dass Bürger:innen frei darüber bestimmen können, wann und an wen die persönlichen Informationen preisgegeben und wie diese Informationen verwendet werden.

2. Dialogkarte „Personenbezogene Daten“

Vorderseite:
Was genau sind personenbezogene Daten?

Rückseite:
Personenbezogene Daten sind Daten, die einer konkreten Person zugeordnet werden können, z.B. Name, Geburtsdatum, Anschrift, Telefonnummer, Kontoauszüge.

Hinweis für das Unterrichtsgespräch:
Personenbezogene Daten müssen unabhängig von der Art ihrer Speicherung (analog oder digital) geschützt werden. Beispielsweise durch einen abschließbaren Aktenschrank oder ein Passwort, dass die Datei schützt.

3. Dialogkarte „Informationelle Selbstbestimmung“

Vorderseite:
Was bedeutet Informationelle Selbstbestimmung?

Rückseite:
Informationelle Selbstbestimmung bedeutet, dass jede Person selbst bestimmen darf, welche persönlichen Daten sie preisgibt und wie ihre persönlichen Daten verwendet werden. Die informationelle Selbstbestimmung ist ein Grundrecht.

Hinweis für das Unterrichtsgespräch:
Personen, die sich in ihrer informationellen Selbstbestimmung beeinträchtigt sehen, weil ihre personenbezogenen Daten von anderen unzulässig preisgegeben oder verwendet werden, können sich vor Gericht wehren. Zugleich muss der Staat in seinem Handeln, beispielsweise bei Erlass eines Gesetzes, das informationelle Selbstbestimmungsrecht seiner Bürger:innen beachten.

4. Dialogkarte „Datenschutzrechtliche Einwilligung“

Vorderseite:
Was ist eine datenschutzrechtliche Einwilligung?

Rückseite:
Eine datenschutzrechtliche Einwilligung ist die Einwilligung, dass eigene persönliche Daten verarbeitet werden dürfen. Wenn man der Verwendung personenbezogener Daten zustimmt, gibt es immer auch Nutzungsbedingungen, wofür diese Daten verwendet bzw. wie sie verarbeitet werden. Diese Bedingungen sind auf der jeweiligen Webseite oder dem Formular vermerkt.

Hinweis für das Unterrichtsgespräch:
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn dies gesetzlich erlaubt ist oder die betroffene Person eingewilligt hat. Eine Einwilligungserklärung kann standardisiert sein, sie muss allerdings freiwillig abgegeben werden. Zudem ist die betroffene Person über den Zweck der Datenerhebung, -verarbeitung und -nutzung, eine geplante Weitergabe der Daten an andere Unternehmen, die Möglichkeit nicht einwilligen zu müssen und die jederzeitige Widerrufsoption zu informieren.

5. Dialogkarte „Datensicherheit / IT-Sicherheit“

Vorderseite:	**Rückseite:**
Was ist Datensicherheit bzw. IT-Sicherheit?	Unter Datensicherheit / IT-Sicherheit versteht man technische oder organisatorische Maßnahmen zum Schutz persönlicher Daten vor Diebstahl, Verfälschung, Missbrauch oder Beschädigung. Dazu zählen z.B. Firewalls, Anti-Viren-Programme und das Verschlüsseln von Daten, aber auch der Gebrauch von verschließbaren Aktenschränken. **Hinweis für das Unterrichtsgespräch:** Ziel der Datensicherheit ist es, dass bestehende Daten nicht beschädigt oder missbraucht werden, z.B. das Daten unverändert bleiben und ausschließlich für autorisierte Personen zugänglich sind.

Anleitung: Digitales Element: Datenschutz-Parcours

Aufgabe

Im digitalen Element sind die Schüler:innen als Roboter Pim oder Nova Teil der Crew auf dem Raumschiff CX3000. Mit einer geführten Steuerung erkunden sie das Raumschiff und treffen dort auf datenschutzrelevante Situationen, in denen sie sich entscheiden müssen, wie sie handeln. Es gibt verschiedene Fragetypen: Multiple-Choice, Freitext und Drag and Drop. Im Anschluss an die Fragen erhalten die Schüler:innen einen allgemeinen „Hinweis von Suni“.

Gesamtauswertung

Wenn die Schüler:innen mit der Bearbeitung des digitalen Elements fertig sind, erhalten sie eine Gesamtauswertung als PDF. Sie dient als Grundlage für das anschließende Unterrichtsgespräch.

Folgende Situationen begegnen den Schüler:innen auf dem Raumschiff. Da wir hier ein reales digitales Spiel simulieren, werden die Schüler:innen mit „du“ angesprochen.

Hinweis: Grüner Punkt 🟢 bedeutet: richtig, Roter Punkt 🔴 bedeutet: falsch.

1. Situation: Transport eines Briefes

Hallo [Pim | Nova], bitte bring diesen Brief zur Versandstelle. Es ist wichtig.

Was musst du beachten?

- 🟢 A) Während ich den Brief transportiere, stelle ich sicher, dass niemand die Details zum Empfänger sehen kann.
- 🟢 B) Ich achte darauf, dass ich den Brief nicht verliere oder er mir sogar gestohlen wird.
- 🔴 C) Wenn der Brief wichtig ist, sollte ich mehr darüber wissen. Ich suche im Internet nach Details zum Empfänger, um mich weiterzubilden.

Hinweis von Suni: Bringe einen Brief immer persönlich und sicher ans Ziel. Lasse ihn nirgendwo liegen und öffne ihn nie. Andere sollten auch die Details zum Empfänger nicht sehen können.

2. Situation: Umgang mit Akten

Obwohl du pünktlich bist, ist dein:e Kolleg:in nicht am Platz. Aber was ist das? Ein Aktenordner mit den Daten-Profilen aller Crew-Mitglieder liegt offen herum.

Was kannst du tun?

- A) Ich schließe den Aktenordner. Es sollten keine personenbezogenen Daten offen herumliegen.
- B) Ich warte ab, bis der:die Kolleg:in wieder da ist und sage, dass personenbezogene Daten nicht offen herumliegen dürfen.
- C) Ich lasse alles, wie es ist. Diese vertraulichen Unterlagen gehen mich nichts an.

Hinweis von Suni: Anschrift und Kontodaten sind personenbezogene Daten und müssen geschützt werden. Bitte lasse sie nie offen herumliegen! Sprich mit deiner:m Kolleg:in. Der Aktenordner sollte zukünftig in einem Schrank aufbewahrt werden.

Vertiefung
Was kann dein:e Kolleg:in künftig tun, um sensible Daten besser zu schützen? Gib praktische Tipps und erkläre, welche Vorteile du darin siehst.

Schreib hier deine Gedanken auf!
(Schüler:innen machen hier eine Freitexteingabe)

Hinweis von Suni: Grundsätzlich gilt: Personenbezogene Daten dürfen nicht offen herumliegen. Bewahre sie so geschützt wie möglich auf. Entweder schließe die Tür ab, sobald du dein Büro verlässt. Oder sperre den Aktenordner in einen Schrank ein. Das gleiche gilt natürlich auch für das offene „Herumliegen“ von digitale Dateien. Diese kann man z.B. mit Passwörtern schützen.

3. Situation: Auffinden von Unterlagen

Gut, dass ich dich hier treffe [Pim / Nova]. Es wäre toll, wenn du vor dem Mittag noch eine Rundmail an unsere Kund:innen in Galaxie 3 rausschickst. Die brauchen die Info, wie viele Lichtjahre wir noch entfernt sind.
(…) Super, du hast die gewünschte Info für die Rundmail bekommen. Oh, da hat wohl jemand nach dem Kopieren ein Arbeitszeugnis verloren.

Wie verhältst du dich?

- A) Ich lese es und gebe es demjenigen, der im Zeugnis beurteilt wird. Es gehört ja schließlich ihm.
- B) Ich lese es und gebe es in der Personalabteilung ab.
- C) Ich schaue an, wer das Zeugnis unterzeichnet hat und bringe es dort vorbei.

Hinweis von Suni: Im Arbeitszeugnis stehen personenbezogene Daten. Wenn du erkennst, wer es erstellt hat, gib es persönlich ab. Sonst informiere deine:n Vorgesetzte:n und schildere deinen Fund.

4. Situation: Versenden von E-Mails

Kapitän Clark hat die Mail für dich bereits vorgeschrieben. Wie nett von ihm! Du musst nur noch die Info zu den Lichtjahren einfügen und sie dann versenden.

Wie verhältst du dich?

- A) Ich setze alle in Kopie (cc) der E-Mail. Transparenz ist wichtig!
- B) Ich schreibe immer alle einzeln an. Persönlicher Kontakt ist am besten.
- C) Ich nutze die Blindkopie-Funktion (bcc). Dann sehen die Empfänger:innen nur die E-Mail-Adresse von mir als Absender:in.

Hinweis von Suni: Nutze die Blindkopie-Funktion (bcc), wenn die Empfänger:innen einer Weitergabe der eigenen E-Mail-Adresse nicht zugestimmt haben oder du nicht weißt, ob sie zugestimmt haben. Die Blindkopie-Funktion spart viel Zeit, weil du nicht jede Person einzeln mit derselben Nachricht anschreiben musst. Achte immer darauf, dass du die Adressen richtig eingibst und die E-Mail nicht an unberechtigte Dritte verschickt wird.

5. Situation: Gespräch mit Dritten

Ist das nicht Valo von deiner letzten Arbeitsstelle? Er hat wohl gerade mit seinem Raumschiff angelegt. Auf welche Frage darfst du antworten und welche solltest du eher unbeantwortet lassen?

Das kann ich beantworten / Richtig:

- Wie viele Leute arbeiten jetzt in der Firma?
- Ist Kapitän Clark immer noch der Big Boss?
- Hast du noch Kontakt mit jemandem aus unserem alten Team?
- Was macht dir am meisten Spaß in deinem Job hier?
- Wie lange ist denn dein Arbeitstag?

Das sollte ich besser nicht beantworten / Falsch:

- Wer verdient bei euch wie viel Gehalt?
- Die Raja aus eurer Crew ist doch wieder schwanger, oder?
- Habt ihr nicht den großen Deal mit der Raumfahrtzentrale abgeschlossen? Wie viel nehmt ihr da ein?
- Welche eurer Kund:innen findest du besonders anstrengend?

Hinweis von Suni: Achte darauf, dass du keine persönlichen Informationen über Kund:innen, Kolleg:innen oder Vorgesetzte nennst. Gib auch keine Geschäfts- und Betriebsgeheimnisse preis.

6. Situation: Verlust von Unterlagen

Oh nein! Du hast deine Raumschiff-Mappe in der Cafeteria liegen-lassen. Darin befindet sich eine Übersicht mit den vertraulichen Daten-Profilen der dir zugeteilten Kund:innen aus Galaxie 3.

Was kannst du tun?

- A) Ich funke den Kantinenroboter an und bitte darum, die Mappe liegen zu lassen, bis ich sie abhole.
- B) Ich gehe gleich in die Kantine zurück und hole die Mappe.
- C) Ich schaue morgen in der Mittagspause nach. Wen sollten schon meine Unterlagen interessieren?

Hinweis von Suni: Die sensiblen Daten sollten so schnell wie möglich gesichert werden. Wenn du nicht selbst hingehen kannst, rufe in der Kantine an und bitte die Angestellten, die Unterlagen sicher bis zur Abholung zu verwahren. Informiere auf jeden Fall deine:n Chef:in über den Vorfall. Es wird dann entschieden, ob die Kund:innen darüber informiert werden müssen.

7. Situation: Anfragen von Daten

Eine Kundin aus Galaxie 4 ist in der Leitung und möchte dringend Zian aus deinem Team sprechen. Sie erreicht ihn aber nicht. Sie bittet dich um die private Handynummer.

Was machst du?

- A) Es ist dringend für die Kundin, also bin ich hilfsbereit und gebe die Handynummer weiter.
- B) Private Nummern gebe ich nie weiter, keine Ahnung ob Zian damit einverstanden ist.
- C) Ich schlage vor, dass ich eine SMS mit der Rückrufbitte an die private Handynummer von Zian schicke. Dann kann Zian selbst entscheiden.

Hinweis von Suni: Gib nie personenbezogene Daten wie private Handy-nummern einfach so weiter. Selbst wenn Zian damit einverstanden wäre, müsstest du prüfen, ob die Anruferin tatsächlich diejenige ist, für die sie sich ausgibt.

8. Situation: Verlassen des Büros

Warte! Du kannst nicht einfach so gehen!! Worauf solltest du achten, wenn du Feierabend machst?

Das kann ich beantworten/Richtig:

- Räume Akten und sonstige Dokumente mit personenbezogenen Daten in einen Schrank.
- Speichere deine digitalen Arbeitsergebnisse des Tages.
- Stelle Maschinen und Geräte aus, die du nicht mehr benötigst.
- Spare Energie und lösche das Licht an deinem Arbeitsplatz.
- Schließe Fenster und Türen.

Das sollte ich besser nicht beantworten / Falsch:

- Nimm Unterlagen mit nach Hause, wenn du die Bearbeitung während der Arbeitszeit nicht geschafft hast.

Hinweis von Suni: Wenn du deinen Arbeitsplatz zum Feierabend verlässt, beachte die Sicherheitsvorkehrungen deines Arbeitgebers. Informiere dich schon am ersten Tag darüber, welche dies sind. Du bist verantwortlich für deinen Arbeitsplatz und ggf. auch die Sicherheit des gesamten Raumschiffs, äh, Firmengeländes oder Büros. Heute hast du dir auf jeden Fall deinen Feierabend verdient. Mach's gut!

Außerdem bearbeiten die Schüler:innen drei Situationen, die am Ende den "Super-Azubi" kühren.

Super-Azubi 1: Verantwortung

Huch! Da ist ja ein riesiger Kaffeefleck am Boden.

Wie verhältst du dich?

- A) Ich gehe weiter und mache einen großen Bogen darum.
- B) So kann das nicht bleiben! Ich wische schnell auf, bevor noch jemand ausrutscht.
- C) Ich mache das Putzpersonal darauf aufmerksam.

Hinweis von Suni: Wunderbar, das ist sehr aufmerksam von dir. Du fühlst dich verantwortlich für die Sauberkeit und Sicherheit an Bord des Raumschiffs. Weiter so!

Super-Azubi 2: Soziales Miteinander

Ahh. Nächste Woche ist ja dein Geburtstag. Das wird bestimmt ein schöner Tag. Hast du schon eine Idee, wie wir den Tag als Team feiern können?

Was wäre eine gute Idee?

- A) Ich verteile meinen Wunschzettel, sodass ich viele Geschenke bekomme.
- B) Ich erkundige mich vorab im Team, ob es Unverträglichkeiten etc. gibt.
- C) Ich bringe leckeren Kuchen und Getränke für alle mit.

Hinweis von Suni: Das ist eine schöne Geste. Als Geburtstagskind gibst du den Anderen etwas aus. Damit niemand leer ausgeht, ist es eine gute Idee, sich vorher zu erkundigen, ob es bei den Anderen Lebensmittelunverträglichkeiten oder bestimmten Ernährungsformen gibt.

Super-Azubi 3: Hilfsbereitsschaft

Ximop sieht ziemlich erschöpft aus. Ob das an dem schweren Koffer liegt?

Was machst du?

- A) Ich frage, ob Ximop Hilfe braucht und biete an, den Koffer zu transportieren.
- B) Ich hab's eilig und bitte Ximop, mir Platz zu machen, damit ich vorbeikomme.
- C) Ich mache mich über Ximop lustig und empfehle ein Fitness-Update!

Hinweis von Suni: Du hast die Situation richtig eingeschätzt und dich respektvoll gegenüber Ximop verhalten.

Tafelbild: Datenschutz im Unternehmensalltag

Das Tafelbild dient zur visuellen Unterstützung für die Reflexionsphase im Anschluss an das digitale Element „Datenschutz-Parcours“. Schlagen Sie die Brücke vom bewusst abstrakt gehaltenen Raumschiff in den konkreten Unternehmensalltag der Schüler:innen.

Anschluss

In der Vorlage finden Sie die acht Parcours-Stationen aus dem digitalen Element. Erarbeiten Sie sie gemeinsam mit den Schüler:innen und übertragen Sie sie in die leeren Felder.

Parcours-Stationen

Lassen Sie die Schüler:innen von persönlichen Erlebnissen in ihrem Arbeitsalltag in einer solchen Situation berichten und erzählen, wie sie gehandelt haben. Verfahren Sie so mit den übrigen sieben Stationen/Situationen.

Persönliche Erlebnisse

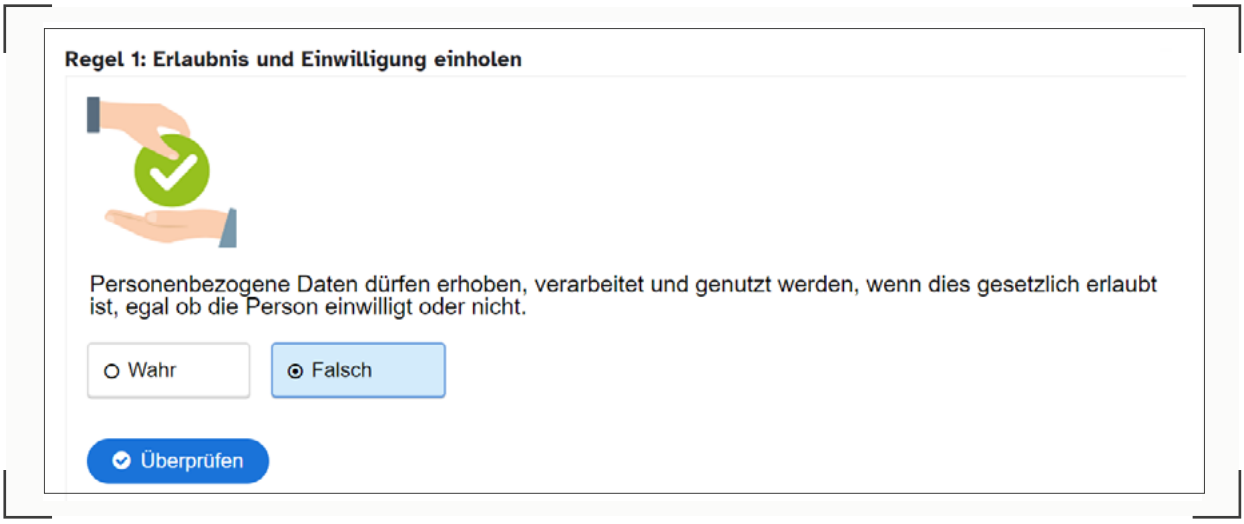
Erstellen Sie bei Bedarf weitere leere Textfelder für den Fall, dass die Schüler:innen mehr als die vorbereiteten acht Situationen nennen.

Eigene Beispiele

Sie können das Tafelbild im Gespräch mit den Schüler:innen an der Tafel entwickeln oder die mebis-Tafel bzw. PowerPoint-Vorlage nutzen.

Weitere Vorlagen

Anleitung: H5P-Tool Check the Paragraphs: Goldene Regeln des Datenschutzes



Aufgabe

Die Schüler:innen absolvieren die Übung in Einzelarbeit. Sie sehen den Namen der Regel ganz oben und prüfen die Formulierung, ob sie richtig oder falsch ist. Insgesamt gibt es sieben Regeln bzw. Aufgaben.

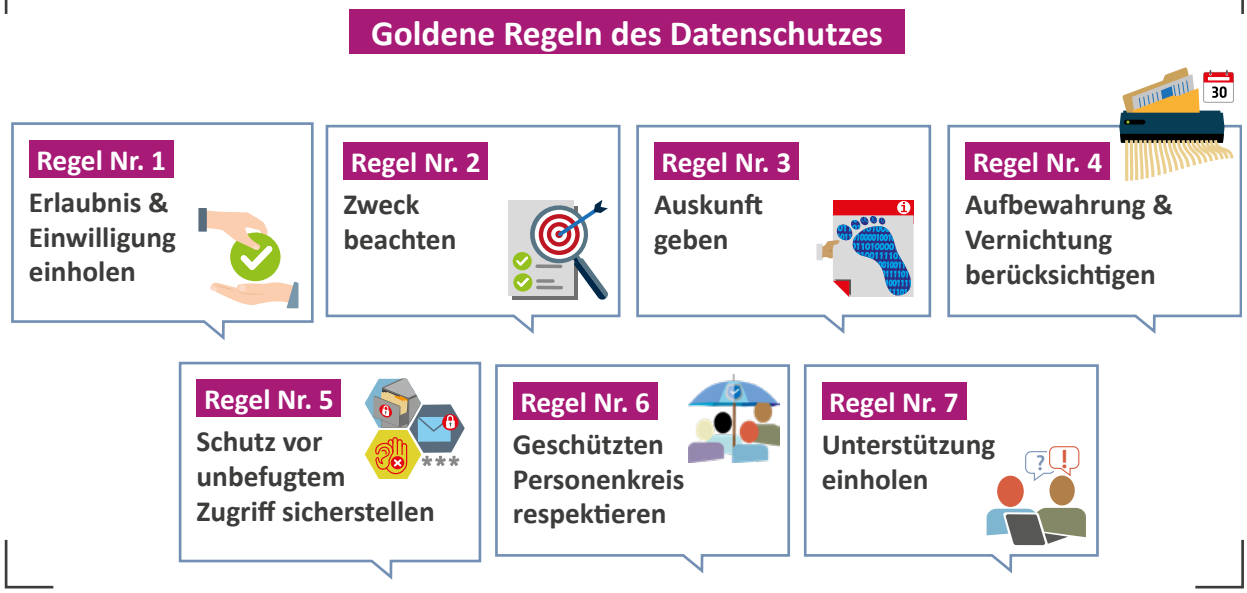
Ziel

Durch das aufmerksame Durchlesen der einzelnen Satzteile prägen sich die Schüler:innen diese allgemeinen Regeln des Datenschutzes ein. In der anschließenden Diskussion können darüber hinaus eigene Regeln aufgestellt werden.

1. Regel	**Erlaubnis und Einwilligung einholen** Personenbezogene Daten dürfen nur erhoben, verarbeitet und genutzt werden, wenn dies gesetzlich erlaubt ist oder die betroffene Person eingewilligt hat.
2. Regel	**Zweck beachten** Personenbezogene Daten dürfen nur für den konkreten Zweck (bzw. die Aufgabe) verwendet werden, für den sie erhoben wurden und nur erhoben werden, wenn diese unbedingt notwendig sind, um den Zweck (bzw. die Aufgabe) zu erfüllen.
3. Regel	**Auskunft geben** Personen dürfen jederzeit Auskunft darüber erhalten, zu welchem Zweck (bzw. für welche Aufgabe) ihre personenbezogenen Daten erhoben und genutzt werden.
4. Regel	**Aufbewahrung und Vernichtung berücksichtigen** Personenbezogene Daten müssen vollständig vernichtet werden, wenn sie nicht mehr gebraucht werden (z.B. wenn der Auftrag abgeschlossen ist) und keine Aufbewahrungs-frist (mehr) besteht.

5. Regel	**Schutz vor unbefugtem Zugriff sicherstellen** Es ist darauf zu achten, dass Unbefugte keinen Zugang zu personenbezogenen Daten haben. Es müssen daher sensible Dokumente z. B. in einem Schrank verschlossen, E-Mails verschlüsselt oder starke Passwörter verwendet werden und es dürfen Unbefugte bei Gesprächen über personenbezogene Daten nicht mithören können.
6. Regel	**Geschützten Personenkreis respektieren** Der Schutz personenbezogener Daten gilt für alle (z.B. für Kund:innen, Patient:innen, Kolleg:innen).
7. Regel	**Unterstützung einholen** Ansprechpartner:innen bei Fragen zum richtigen Umgang mit personenbezogenen Daten sind Ausbildungsleiter:innen und Vorgesetzte. Falls diese Unterstützung brauchen, können sie sich an betriebliche Datenschutzbeauftragte wenden (sofern vorhanden).

Tafelbild: Goldene Regeln des Datenschutzes



Ziel

Die gemeinsame Erstellung des Tafelbilds „Regeln" nach der Einzelübung „Check The Paragraphs" dient dazu, die Regeln zu festigen und den Schüler:innen Raum für Reflexion und Nachfragen zu geben.

Aufgabe

In der Vorlage finden Sie die Titel der sieben „Goldenen Regeln des Datenschutzes" aus der eben absolvierten Einzelarbeit. Übertragen Sie die Regeln in die jeweiligen Textfelder. Fordern Sie die Schüler:innen auf, die einzelnen Regeln zu erläutern. Geben Sie bei Bedarf Hilfestellung und antworten Sie auf Nachfragen.

Erstellen Sie bei Bedarf weitere leere Textfelder für den Fall, dass die Schüler:innen eigene Regeln aufstellen möchten.

Konsequenzen

Lassen Sie die Schüler:innen über mögliche Konsequenzen diskutieren, die sich aus der Nichtbeachtung von Datenschutzregeln ergeben könnten und geben Sie Hinweise auf tatsächliche (berufliche und strafrechtliche) Konsequenzen bei Datenschutzverletzungen.

Weitere Vorlagen

Sie können das Tafelbild im Gespräch mit den Schüler:innen an der Tafel entwickeln oder die mebis-Tafel bzw. PowerPoint-Vorlage nutzen.

Merkblatt: Goldene Regeln des Datenschutzes

Der Begriff **Datenschutz** umfasst den rechtlichen Schutz persönlicher Daten. Weil diese Daten einer bestimmten Person zugeordnet werden können, werden sie auch als **personenbezogene** Daten bezeichnet (z.B. Name, Geburtsdatum, Adresse, Hautfarbe, Kontodaten). Folgende Datenschutzregeln sind im Arbeitsalltag hilfreich.

Erlaubnis und Einwilligung

Personenbezogene Daten dürfen nur erhoben, verarbeitet und genutzt werden, wenn

» dies gesetzlich erlaubt ist oder

» die betroffene Person eingewilligt hat.

Zweck

Personenbezogene Daten dürfen

» nur für den konkreten Zweck (bzw. die Aufgabe) verwendet werden, für den sie erhoben wurden und

» nur erhoben werden, wenn diese unbedingt notwendig sind, um den Zweck (bzw. die Aufgabe) zu erfüllen.

Auskunft

Personen dürfen jederzeit Auskunft darüber erhalten, zu welchem Zweck (bzw. für welche Aufgabe) ihre personenbezogenen Daten erhoben bzw. genutzt werden.

Schutz vor unbefugtem Zugriff

Es ist darauf zu achten, dass Unbefugte keinen Zugang zu personenbezogenen Daten haben.

» Es müssen daher sensible Dokumente z. B. in einem Schrank verschlossen, E-Mails verschlüsselt oder starke Passwörter verwendet werden und

» es dürfen Unbefugte bei Gesprächen über personenbezogene Daten nicht mithören können.

Geschützter Personenkreis

Der Schutz personenbezogener Daten gilt für alle (z. B. für Kund:innen, Patient:innen, Kolleg:innen).

Aufbewahrung und Vernichtung

Personenbezogene Daten müssen vollständig vernichtet werden, wenn

» sie nicht mehr gebraucht werden (z. B. wenn der Auftrag abgeschlossen ist) und

» keine Aufbewahrungsfrist (mehr) besteht

Unterstützung

Ansprechpartner:innen bei Fragen zum richtigen Umgang mit personenbezogenen Daten sind

» Ausbildungsleiter:innen und

» Vorgesetzte.

Falls diese Unterstützung brauchen, können sie sich an betriebliche Datenschutzbeauftragte wenden (sofern vorhanden).

Information: Grundlagen des Datenschutzes

Definition

Der Begriff des Datenschutzes umfasst den rechtlichen Schutz persönlicher Daten. Regelungen dazu ergeben sich aus Gesetzen, Verordnungen oder der Rechtsprechung. Von großer Bedeutung ist daneben die Datensicherheit, auch IT-Sicherheit genannt. Die Datensicherheit meint alle Maßnahmen technischer oder organisatorischer Art, die einem eventuellen Datenmissbrauch, also dem Löschen, Verfälschen oder Diebstahl von Daten, vorbeugen sollen. [1]

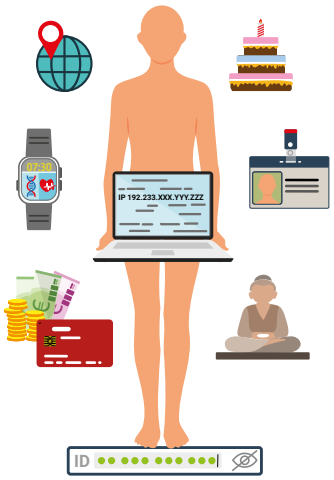
Informationelle Selbstbestimmung

Das zentrale Ziel der datenschutzrechtlichen Regelungen besteht darin, die Privatsphäre der Einzelnen zu schützen und ihnen die Möglichkeit zu verschaffen, frei über die Veröffentlichung und Verwendung ihrer persönlichen Daten bestimmen zu können. Dieses Recht auf informationelle Selbstbestimmung ist eine Ausprägung des allgemeinen Persönlichkeitsrechts, das jedem Menschen die freie Entfaltung seiner Persönlichkeit ermöglichen soll und gleichzeitig die Privatsphäre des Einzelnen schützt.

Die wichtigsten Bestimmungen zum Datenschutz finden sich in Deutschland im Bundesdatenschutzgesetz (BDSG), das für Bundesbehörden und Unternehmen gilt, und in den weitgehend gleichlautenden Landesdatenschutzgesetzen, die für die Landesbehörden gelten. Daneben gibt es für spezielle Bereiche eigene datenschutzrechtliche Gesetze, wie z. B. das Telekommunikationsgesetz oder das Telemediengesetz. Zudem gilt ab Mai 2018 auf europäischer Ebene die Datenschutz-Grundverordnung, die in allen Mitgliedstaaten der Europäischen Union zu beachten ist.

Personenbezogene Daten

Das Datenschutzrecht schützt sogenannte personenbezogene Daten. Damit sind Daten gemeint, die einen konkreten Bezug zu einer Person zulassen. Dabei spielt es keine Rolle, ob die Daten auch den Namen der Person beinhalten. Selbst ohne Angabe des Namens können sich Daten einer konkreten Person zuordnen lassen. Personenbezogene Daten werden unabhängig von der Art ihrer Speicherung (analog oder digital) geschützt. Personenbezogene Daten sind beispielsweise Name, Geburtsdatum, Anschrift, Telefonnummer, Kontoauszüge oder Hautfarbe.



Mitarbeiter:innen und Auszubildende kommen in ihrem Beruf täglich mit personenbezogenen Daten in Kontakt. Wenn diese Daten eine bestimmte oder bestimmbare Person betreffen, handelt es sich um sogenannte personenbezogene Daten. Das können beispielsweise persönliche Daten von Kund:innen, Kolleg:innen, Lieferant:innen oder Gästen sein. Beim Umgang mit diesen personenbezogenen Daten (z. B. beim E-Mail-Kontakt mit Lieferanten oder beim Umgang mit Kundendaten am PC) sind die Regelungen des Datenschutzrechts zu beachten.

Datenspeicherung

Damit ein Auftrag bewältigt werden kann, müssen Unternehmen personenbezogene Daten von Kund:innen erheben. Die meisten Mitarbeiter:innen kommen daher mit personenbezogenen Daten in Kontakt. Die personenbezogenen Daten werden zur Erfüllung des Auftrages oder der behördlichen Aufgabe in analoger oder digitaler Form erfasst, aufgenommen oder aufbewahrt – und damit gespeichert.

Datenverarbeitung

Der Begriff Datenverarbeitung dient als Oberbegriff für das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Damit beschreibt er nahezu jeden automatisierten und nicht-automatisierten Vorgang im Zusammenhang mit personenbezogenen Daten.

Verwendung der Daten

Unternehmen, Behörden und andere Einrichtungen dürfen personenbezogene Daten nicht einfach für sich nutzen (z. B. für gezielte Werbung). Sie müssen sich an die datenschutzrechtlichen Vorgaben halten und beim Umgang mit personenbezogenen Daten verschiedene Grundsätze beachten. So ist beispielsweise gesetzlich festgelegt, dass personenbezogene Daten nur für einen bestimmten Zweck erhoben und nicht anderweitig verwendet werden dürfen. Werden die Regelungen nicht eingehalten, drohen Schadensersatzforderungen oder Strafen wie z. B. Bußgelder.

Geschäfts- und Betriebsgeheimnisse

Neben den personenbezogenen Daten gibt es in Unternehmen noch andere sensible Daten, die man als Geschäfts- und Betriebsgeheimnisse bezeichnet. Geschäfts- und Betriebsgeheimnisse sind beispielsweise Informationen zum Umsatz, zur Kostenverteilung, zur Forschung und Entwicklung, zur Werbestrategie, zu Vertragsdetails, zu Produktionsschritten, zu internen Anweisungen oder zu Arbeitsvorgängen.

Schutz sensibler Daten

Soweit Geschäfts- und Betriebsgeheimnisse keinen Personenbezug aufweisen, werden sie nicht durch das Datenschutzrecht geschützt, da dieses nur personenbezogene Daten erfasst. Geschäfts- und Betriebsgeheimnisse werden stattdessen durch andere Regelungen, wie z. B. das Straf- und das Lauterkeitsrecht, geschützt. Da Geschäfts- und Betriebsgeheimnisse regelmäßig Informationen umfassen, deren Veröffentlichung für Unternehmen von wirtschaftlichem Nachteil sein könnten, haben die Unternehmen selbst ein großes Interesse daran, solche Betriebsdaten zu schützen.

Unternehmensgröße

Die Größe eines Unternehmens spielt beim Datenschutz keine Rolle. Unternehmen, Behörden und auch Selbstständige haben die datenschutzrechtlichen Bestimmungen unabhängig von der Anzahl der Mitarbeiter:innen zu beachten. Grundsätzlich muss die Unternehmensleitung dafür sorgen, dass die datenschutzrechtlichen Vorgaben von allen Angestellten eingehalten werden. Datenschutz ist auch bedeutsam für das Vertrauen der Kund:innen sowie der Geschäftspartner:innen in ein Unternehmen.

Information: Bedeutung des Datenschutzes

Digitale Revolution

Seit Anfang der 1990er Jahre haben sich die Informations- und Kommunikationsmöglichkeiten für einen Großteil der weltweiten Bevölkerung erheblich verändert. Dieser Prozess, der durch die Erfindung des Mikrochips, den massentauglichen Einsatz von Computern und die flächendeckende Verbreitung des Internets in Gang gesetzt wurde, wird auch als digitale Revolution bezeichnet. Seither werden Informationen in immer größerem Umfang digital verarbeitet und ausgewertet. [2]

Einfluss auf unser Alltagsleben

Der Einfluss der digitalen Revolution reicht in nahezu alle Lebensbereiche. So sind Computer oder Smartphones im privaten und beruflichen Bereich heute kaum mehr wegzudenken. Viele Geräte, die wir im Alltag benutzen, sind mittlerweile digital vernetzt. Dazu gehören Telefone, Autos, Rasensprenger, Stromzähler, Kleidung, Fitnessarmbänder und Brillen. Die letzten drei Beispiele bezeichnet man als sogenannte „Wearables“, also Computersysteme, die man am Körper trägt. Zukünftig werden Geräte stärker als bisher untereinander kommunizieren können. Dies wird als „M2MKommunikation“ (Machine to Machine-Kommunikation) bezeichnet. [3]

Für den Staat bietet sich durch die Digitalisierung die Möglichkeit, z. B. Verwaltungsverfahren wie etwa das Einreichen einer Steuererklärung oder das Beantragen eines Kita-Platzes, online abzuwickeln. Auch die Wirtschaft verändert sich durch die digitale Revolution. Das Schlagwort „Industrie 4.0“ beschreibt die engere Verzahnung von Produktion, Logistik und Kundenwünschen mit Hilfe digital vernetzter, intelligenter Systeme. [9]

Zugleich ergeben sich durch die Digitalisierung Herausforderungen, insbesondere bei der Abwehr von sogenannten Cyberattacken. Cyberattacken sind von außen zum Zweck der Sabotage oder der Informationsgewinnung geführte Angriffe auf Computernetzwerke. Sie können dazu führen, dass geheime Dokumente gestohlen werden oder wichtige Infrastruktur zusammenbricht wie z. B. Energie- oder Verkehrsnetze. [4]

Steigende Datenmengen

Infolge der technischen Entwicklung ist die Menge der gespeicherten und verfügbaren Daten enorm gewachsen. Daten können beim Surfen, Chatten, Telefonieren, E-Mail-Schreiben, Fernsehen, Autofahren, Online-Banking oder bei der Nutzung technischer Geräte wie z. B. Navigationssysteme oder Pulsmesser erfasst und anschließend ausgewertet und verarbeitet werden.

Big Data

Die Menge vorhandener Daten, die im Zuge der fortschreitenden Digitalisierung weltweit kontinuierlich wächst, wird auch als Big Data bezeichnet. Die schiere Größe der Datenmenge und die Schnelligkeit, mit der diese weiter anwächst, führt bei der Datenverarbeitung zum einen zu völlig neuen Anwendungsmöglichkeiten und zum anderen zu einer Komplexität, die mit bisherigen Verarbeitungsmethoden nur bedingt bewältigt werden kann.

Auswertung großer Datenmengen

Mit dem Begriff Big Data werden auch Verfahren zur automatisierten Auswertung großer Datenmengen verknüpft. Um Aussagen über die statistische Wahrscheinlichkeit bestimmter zukünftiger Entwicklungen treffen zu können, werden IT-Lösungen und spezielle Programme genutzt. Diese Big Data-Verfahren erlauben es, z. B. Prognose- oder Frühwarnsysteme aufzubauen, um bevorstehende Epidemien oder gefährliche Wetterlagen zu erkennen.

Big Data im Unternehmen

Auch einige Unternehmen nutzen diese Verfahren z. B. zur gezielten Werbung. Die technische Entwicklung erlaubt es mittlerweile, auf Grundlage von Daten, die z. B. aus der Nutzung von Social-Media-Angeboten stammen, das zukünftige Nutzerverhalten vorherzusagen. Das betrifft nicht nur eventuelle Online-Käufe oder Produktwünsche, sondern beispielsweise auch den voraussichtlichen Standort einer Person zu einem bestimmten Zeitpunkt. [5]

Spannungsverhältnis

Da personenbezogene Daten von Kund:innen eine gezieltere Werbung und eine genauere Einschätzung des Konsumverhaltens zulassen und damit ein äußerst wertvolles Gut für Unternehmen sind, kann ein Spannungsverhältnis zwischen den wirtschaftlichen Interessen von Betrieben und dem Schutz von Kundendaten entstehen. Auch wenn manche Unternehmen gerne so viele personenbezogene Daten wie möglich erheben, verarbeiten und nutzen möchten, ist dies laut Datenschutzrecht nicht zulässig. Auch die Weitergabe von Daten an Dritte ist nicht ohne Einwilligung der:des Betroffenen erlaubt.

Gläserner Mensch

Je mehr Daten über einen Menschen vorliegen, desto leichter kann sein Verhalten analysiert und vorhergesagt werden. Denn personenbezogene Daten ermöglichen Rückschlüsse auf alle Lebensgewohnheiten eines Menschen. Dieses Phänomen wird mit dem Schlagwort des gläsernen Menschen bezeichnet. Dies kann beispielsweise negative Auswirkungen haben, wenn aus statistischen Wahrscheinlichkeiten Rückschlüsse über den einzelnen Menschen gezogen werden. Es ist z. B. möglich, dass allein aus dem Umstand, in welchem Stadtteil eine Person wohnt, auf ihre Kreditwürdigkeit geschlossen wird.

Bedeutung des Datenschutzes

Um die Privatsphäre der Einzelnen zu schützen und ihnen die Möglichkeit zu verschaffen, sich frei von äußeren Einflüssen entfalten zu können, müssen Betroffene grundsätzlich selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten bestimmen können. Wäre die freie Entfaltung der eigenen Persönlichkeit und der Schutz der Privatsphäre nicht gegeben, bestünde die Gefahr, dass Einzelne ihr Handeln nicht auf freier Willensbildung gründen, sich also fremdbestimmt verhalten.

Bedeutung für die Demokratie

In einem solchen Fall könnten Einzelne auch nicht mehr selbstbestimmt und frei an der politischen Willensbildung und dem Wirtschaftsleben teilhaben. Denn wenn Personen die Entscheidungsfreiheit darüber verlieren, wer was wann über sie weiß, kann dies dazu führen, dass sie sich möglichst „stromlinienförmig“ verhalten wollen, also z. B. nicht an Bürgerinitiativen oder öffentlichen Versammlungen teilnehmen, um nicht negativ aufzufallen. Mögliche Folgen können sein, dass es weniger öffentliche Debatten gibt und wichtige Argumente unausgesprochen bleiben. Es ist beispielsweise möglich, dass Missstände ungenügend kritisiert werden würden. Dies würde sowohl die individuellen Entfaltungschancen beeinträchtigen, als auch der Grundidee der freiheitlichen Demokratie widersprechen, die auf die Mitwirkung ihrer Bürger:innen angewiesen ist.

Selbstdatenschutz

Die Konsequenzen der Preisgabe personenbezogener Daten durch Betroffene selbst oder Unternehmen lassen sich zum Teil nicht im Vorhinein absehen. Einige Menschen veröffentlichen jedoch im Internet mit dem Argument, dass sie nichts zu verbergen haben, viel mehr persönliche Informationen als sie Fremden in der Realität zugänglich machen würden. Gelegentlich werden Daten auch unbewusst preisgegeben, etwa wenn bei der Nutzung bestimmter Angebote oder beim Einkaufen im Internet die Datenschutzrichtlinien akzeptiert werden, ohne sie durchzulesen. Alle Menschen sollten sich aber bewusst machen, dass veröffentlichte Daten für jedermann zugänglich sind und oftmals nur schwer bis gar nicht vollständig gelöscht werden können. [6]

Information: Pflichten von Unternehmen

Zulässiger Umgang mit Daten

Der Umgang mit personenbezogenen Daten innerhalb eines Unternehmens ist nur dann zulässig, wenn er entweder durch die Gesetze erlaubt wird oder eine Einwilligung der betroffenen Person vorliegt. Bei Online-Händlern wird die Einwilligungserklärung häufig dadurch erteilt, dass Kund:innen die Nutzungsbedingungen bzw. die Allgemeinen Geschäftsbedingungen (AGB) und die Datenschutzerklärung akzeptieren.

Unternehmen müssen beim Umgang mit personenbezogenen Daten verschiedene Grundsätze beachten. So sind sie beispielsweise an den Grundsatz der Datenvermeidung und Datensparsamkeit gebunden. Das bedeutet, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten sind, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Das bedeutet, dass z. B. ein Online-Händler nur so viele personenbezogene Daten abfragen darf, wie er für die Zusendung des Produkts benötigt (z. B. Namen, Lieferadresse und Telefonnummer, nicht aber Religionszugehörigkeit). Dazu gehört auch, dass personenbezogene Daten sofort zu löschen sind, wenn der mit ihnen verbundene Zweck erreicht wurde und sie nicht mehr für diesen Zweck gebraucht werden.

Aufbewahrungspflichten

Personenbezogene Daten dürfen jedoch nicht gelöscht werden, wenn gesetzliche Aufbewahrungspflichten bestehen wie z. B. bei Akten von Patient:innen oder analogen und digitalen Bewerbungsdokumenten. Besteht eine solche Frist, müssen die Daten derart gesichert werden, dass der Zugriff der Mitarbeiter:innen sowie Dritter auf diese Daten für andere Zwecke ausgeschlossen ist.

Grundsatz der Zweckbindung

Darüber hinaus müssen Unternehmen den Grundsatz der Zweckbindung beachten. Dieser Grundsatz besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Wenn ein Online-Händler beispielsweise personenbezogene Daten für das Zusenden eines Produkts erfasst, darf er diese Daten nicht für einen anderen Zweck verwenden, wie z. B. für das Zusenden eines Newsletters. Hierfür muss er eine weitere Einwilligung einholen.

Grundsatz der Transparenz

Der Grundsatz der Transparenz bedeutet, dass Betroffene einen Anspruch darauf haben, zu erfahren, ob und wie die personenbezogenen Daten verarbeitet werden. Daraufhin können Betroffene die Daten berichtigen, löschen oder bei noch bestehenden Aufbewahrungsfristen sperren lassen. Wenn eine Kundin beispielsweise bei einem Online-Händler ein Produkt bestellt, kann sie nachfragen, wofür ihre personenbezogenen Daten verwendet werden. Der Online-Händler muss sie dann über die Verarbeitung ihrer personenbezogenen Daten informieren (insbesondere über Art, Umfang und Zweck).

Wenn die Kundin damit nicht einverstanden ist, hat sie die Möglichkeit, ihre Daten z. B. löschen zu lassen.

Pflicht zur Datensicherheit

Unternehmen müssen die Sicherheit der Daten gewährleisten und technische und organisatorische Maßnahmen treffen, die zur Sicherstellung des Datenschutzes erforderlich sind. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Als verhältnismäßig kann im Bereich der digitalen Datensicherung z. B. der Einsatz von Verschlüsselungsverfahren, Antivirenprogrammen und Firewalls angesehen werden.

Datenschutzbeauftragte

Ferner sind Unternehmen verpflichtet, gemäß der gesetzlichen Vorgabe eine:n Datenschutzbeauftragte:n zu bestellen. Als Datenschutzbeauftragte können vom Unternehmen sowohl eigene Mitarbeiter:innen mit entsprechenden Kenntnissen als auch externe, fachkundige Personen bestellt werden. Betriebliche Datenschutzbeauftragte sorgen für die Einhaltung der datenschutzrechtlichen Bestimmungen im Unternehmen. Sie verfügen über das entsprechende Wissen und die Verantwortung, den Mitarbeiter:innen bei Fragen zum Umgang mit personenbezogenen Daten zu helfen. Zugleich prüfen sie die Arbeitsvorgänge, um z. B. fahrlässige Datenschutzverstöße von Angestellten zu verhindern. [7]

Information: Pflichten von Arbeitnehmer:innen

Datenschutzrechtliche Verpflichtungen für Mitarbeiter:innen ergeben sich nicht nur aus den Datenschutzgesetzen, sondern in der Regel auch aus dem Arbeitsverhältnis. Für gewöhnlich enthält der Arbeitsvertrag eine sogenannte Verschwiegenheitserklärung, welche Mitarbeiter:innen zur Wahrung des Datengeheimnisses und zumeist auch zur Wahrung des Geschäftsgeheimnisses verpflichtet. Aufgrund dieser und weiterer gesetzlicher Verpflichtungen dürfen Mitarbeiter:innen personenbezogene Daten und Geschäfts- und Betriebsgeheimnisse nicht an andere weitergeben – oftmals nicht einmal an Kolleg:innen. Missachten Angestellte diese Vorgaben, müssen sie (insbesondere) mit arbeitsrechtlichen Konsequenzen und Schadensersatzforderungen rechnen.

Pflichten am Arbeitsplatz

Im Arbeitsalltag müssen Mitarbeiter:innen im Rahmen ihrer Möglichkeiten dafür Sorge tragen, dass sensible Daten ausreichend gesichert werden. Dies betrifft sowohl Akten als auch personenbezogene Daten, die digital gespeichert sind. Befinden sich die Daten auf einem Firmen-PC, so ist dieser z. B. mit einem ausreichend sicheren Passwort zu versehen (mindestens acht Zeichen, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen). Akten mit personenbezogenen Daten sollten nach dem Gebrauch in einem Schrank eingeschlossen werden.

Pflichten beim Transport sensibler Daten

Auch beim Transport sensibler Daten müssen Sicherheitsvorkehrungen getroffen werden. Es empfiehlt sich, Dokumente nicht lose mit sich zu führen oder abzulegen, sondern diese geschlossen in einer Tasche aufzubewahren. Auch USB-Sticks oder Laptops sollten in einer Tasche transportiert werden. Mitarbeiter:innen sollten die Taschen stets bei sich tragen und nicht aus den Augen lassen.

Pflichten beim E-Mail-Verkehr

Im E-Mail-Verkehr ist darauf zu achten, bei E-Mails, die an mehrere externe Empfänger:innen gerichtet sind (z. B. Kunden-Newsletter oder Elternbriefe), die Blindkopie-Funktion (bcc) zu nutzen. Dann sehen die Empfänger:innen nur die E-Mail-Adresse der Absender:innen, nicht jedoch die anderen Empfänger:innen. Dies gilt immer dann, wenn die Empfänger:innen einer Weitergabe der eigenen E-Mail-Adresse (zumindest für diesen Zweck) nicht zugestimmt haben.

Pflichten beim Gespräch

In der mündlichen Kommunikation müssen sowohl im beruflichen als auch im privaten Kontext ebenfalls die Sorgfaltspflichten des Datenschutzrechts eingehalten werden. Angestellte müssen in Gesprächen darauf achten, keine Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person preiszugeben. In der telefonischen oder persönlichen Kommunikation mit Kund:innen muss beim Austausch solcher Angaben garantiert sein, dass andere Personen nicht mithören können (z. B. durch das Senken der Stimme).

Pflichten beim Vernichten von Daten

Beim Löschen bzw. dem Vernichten von personenbezogenen Daten müssen Mitarbeiter:innen darauf achten, dass diese Daten nicht in fremde Hände geraten. Daher ist es beispielsweise notwendig, beim Vernichten von Dokumenten mit personenbezogenen Daten einen Aktenvernichter zu benutzen und sie nicht in den Papierkorb zu entsorgen. [8]

Verhalten bei Verstößen

Kommt es wissentlich oder unwissentlich zu einem Verstoß gegen die Datenschutzbestimmungen, ist dieser umgehend zu beseitigen. Bemerken Mitarbeiter:innen, dass sich Kolleg:innen nicht datenschutzrechtskonform verhalten, sind diese darauf hinzuweisen. Bei mehrmaligen Verstößen sollten die Ausbildungsleiter:innen oder die Vorgesetzten informiert werden. Stellen Mitarbeiter:innen fest, dass Fremde unrechtmäßig in den Besitz sensibler Daten gekommen sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, sollten unverzüglich Ausbildungsleiter:innen oder Vorgesetzte informiert werden. Diese können sich gegebenenfalls an die oder den Datenschutzbeauftragten des Betriebs wenden. Datenschutzbeauftragte oder Vorgesetzte sind zur unmittelbaren Mitteilung an die zuständige Aufsichtsbehörde (in der Regel das entsprechende Landesamt für Datenschutz) sowie die oder den Betroffenen verpflichtet.

Folgen bei Verstößen

Die Missachtung datenschutzrechtlicher Vorgaben kann, selbst wenn dies unabsichtlich geschieht, für Mitarbeiter:innen arbeitsrechtliche und finanzielle Folgen haben. Ist ein fahrlässiger Verstoß gegen datenschutzrechtliche Bestimmungen nachzuweisen, kann dies in leichten Fällen zu Ermahnungen, in schwerwiegenderen Fällen zu einer (fristlosen) Kündigung führen. Dazu kann ein Bußgeld von Seiten der zuständigen Aufsichtsbehörde ausgesprochen werden. Handelte die:der Mitarbeiter:in in voller Absicht, kann dies sogar im Einzelfall zu einem Strafverfahren führen. Der betreffenden Person droht dann eine Geldstrafe oder eine Freiheitsstrafe von bis zu zwei Jahren. Um nicht selbst für das Fehlverhalten ihrer Mitarbeiter:innen bestraft zu werden, müssen Vorgesetzte ihrer Aufsichtspflicht nachkommen und ein datenschutzrechtskonformes Verhalten aller Mitarbeiter:innen sicherstellen (z. B. durch entsprechende Arbeitsanweisungen und regelmäßige Überprüfung). [9]

Quellenangaben

[1] Karg, Moritz. In: Wolff, Heinrich A./Brink, Stefan (Hrsg.): BeckOK Datenschutzrecht. 20. Ed. Stand 01.05.2017, BDSG § 9, Rn. 8-10.

[2] Jacobi, Hans-Friedrich/Landherr, Martin (2013): Bedeutung des Treibers Informations-und Kommunikationstechnik für die Wettbewerbsfähigkeit industrieller Produktion. In: Westkämper, Engelbert/Spath, Dieter/Constantinescu, Carmen/Lentes, Joachim (Hrsg.): Digitale Produktion. Heidelberg: Springer Vieweg, S. 41-44.

[3] Wilmer, Stefan (2016): Wearables und Datenschutz – Gesetze von gestern für die Technik von morgen? In: Kommunikation und Recht (K&R), H. 6/2016, S. 382-389.

[4] Heesen, Jessica (2016) (Hrsg.): Handbuch Medien- und Informationsethik. Stuttgart: J.B. Metzler.

[5] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RLP): Big Data. Internet: www.youngdata.de/internet/big-data/ [Stand: 19.11.2022].

[6] Specht, Louisa (2016): Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen. Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung. In: CR, H. 5/2016, S. 288-296.

[7] Brandt, Jochen. In: Hauschka, Christoph E./Moosmayer, Klaus/Lösler, Thomas (Hrsg.): Corporate Compliance. Handbuch der Haftungsvermeidung in Unternehmen. München: C.H. Beck. 3. Auflage 2016, § 29, Rn. 13-21.

[8] Stiftung Datenschutz (Hrsg.): Datenschutz ganz kurz. Was Beschäftigte unbedingt wissen sollten. Internet: www.stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Broschuere/SDS_Datenschutz_ganz_kurz_allgemein_2022-12_DE_Web.pdf [Stand: 19.11.2022].

[9] Stiftung Datenschutz (2016): Datenschutz im Betrieb. Eine Handreichung für Beschäftigte. Internet: www.stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Broschuere/SDS_Datenschutz_im_Betrieb_SDS_2022-12_DE_Web.pdf [Stand: 19.11.2022].

[10] Ackermann, Astrid: Mitarbeiter Schulung – Vorteil beim Datenschutz? In: Datenschutzbeauftragter INFO, 18. November 2015. Internet: www.datenschutzbeauftragter-info.de/mitarbeiter-schulung-vorteil-beim-datenschutz/ [Stand: 19.11.2022].

Impressum

Konzeption: Stiftung Medienpädagogik Bayern und KIDS interactive GmbH
Redaktion: Jutta Baumann, Lina Renken, Amelie Hofmann und Simone Hirschbolz
Lehrplanbezug: Staatsinstitut für Schulqualität und Bildungsforschung (ISB)

Die Medienführerschein Werkstatt basiert auf der Unterrichtseinheit „Viele Daten, viel Verantwortung! Datenschutzrechtliche Grundlagen verstehen und im Arbeitsalltag anwenden“ des Medienführerscheins Bayern für Berufliche Schulen
(2. überarbeitete Auflage).

Autor:innen des Moduls „Viele Daten, viel Verantwortung“: Prof. Dr. Anne Lauber-Rönsberg, Philipp Krahn, Manuela Liebig (Technische Universität Dresden)
Satz/Layout: Helliwood media & education
Illustrationen: Peter Weber Grafikdesign
Digitales Element “Datenschutz-Parcours”: KIDS interactive GmbH

Bayerisches Staatsministerium für Unterricht und Kultus

Entwicklung der Materialien gefördert durch das Bayerische Staatsministerium für Unterricht und Kultus.

München, Dezember 2022