

LAP Fragenkatalog - IT Systemtechniker/Betriebstechniker

- LAP Fragenkatalog - IT Systemtechniker/Betriebstechniker
- 1. Allgemeiner Teil - Informationstechnologie
 - 1.1 Ergonomische Gestaltung eines Arbeitsplatzes
 - 1.1.1 Ergonomische Einrichtung eines Bildschirmarbeitsplatzes
 - 1.1.2 Optimaler Aufstellungsort von Bildschirmen (Lichteinfall)
 - 1.1.3 Gesetzliche Bestimmungen von Pausen bei Bildschirmarbeit
 - 1.1.4 Schutzmaßnahmen und körperliche Entspannungsübungen
 - 1.2 Arbeitssicherheit und Schutzmaßnahmen
 - 1.2.1 Arbeitssicherheit und Schutzmaßnahmen
 - 1.2.2 Kenntnisse über Wirkungsweise und Gefahren des elektrischen Stroms
 - Mensch im Stromkreis
 - Gesetze und Vorschriften
 - Elektroschutzkonzept
 - Schutz gegen direktes Berühren - Basisschutz
 - Schutz bei indirektem Berühren - Fehlerschutz
 - Schutzklassen elektrischer Geräte
 - 1.2.3 Kenntnisse über Verhalten und Maßnahmen bei einem Elektrounfall (Reihenfolge)
 - Rettungsvorgang
 - Zusätzliche Sicherheitshinweise:
 - 1.2.4 Kenntnisse über Gefahren bei einem Brand und richtiges Verhalten beim Brandfall (Reihenfolge)
 - 1.2.5 Kenntnisse über CO₂- und Pulver-Feuerlöscher
 - 1.2.6 Richtige Verwendung von Feuerlöschern bei elektrischen Anlagen
 - 1.2.7 Richtiger Umgang und korrekte Lagerung von Akkus oder Batterien
 - 1.2.8 Kenntnisse über umweltgerechte Entsorgung von Elektronikschrott, Toner, Akkus oder Batterien
 - 1.2.9 Kenntnisse über arbeitsrechtliche Gesetze (KJBG, ASchG, GIBG)
 - 1.3 Technische Dokumentation
 - 1.3.1 Aufgabe und Strukturierung von Testläufen
 - 1.3.2 Inhalt einer technischen Dokumentation/eines technischen Protokolls
 - 1.3.3 Aufbereitung einer technischen Dokumentation/eines technischen Protokolls
 - 1.3.4 Anwendung der Schrittaufzeichnung/Step Recorder
 - 1.3.5 Beilagen technischer Dokumentationen (Testprotokoll, Netzwerkplan, ...)
 - 1.3.6 Gestaltung und Vorbereitung von Präsentationen
 - 1.4 Datenschutzgrundverordnung (DSGVO)
 - 1.4.1 Aktuelle DSGVO
 - 1.4.2 Datenminimierung
 - 1.4.3 Fachbegriffe laut DSGVO
 - 1.4.4 Rechte von betroffenen Personen
 - 1.4.5 Personenbezogene und sensible Daten
 - 1.4.6 Kopplungsverbot

- 1.4.7 Datenschutzbeauftragter
- 1.4.8 Pflichten bei Datendiebstahl
- 1.4.9 Weitere rechtliche Grundlagen
- 1.5 Fachbegriffe und Grundlagen in der Informationstechnik
 - 1.5.1 Fachbegriff Big Data
 - 1.5.2 Fachbegriff Web 2.0
 - 1.5.3 Fachbegriff Industrie 4.0
 - 1.5.4 Fachbegriff IoT (Internet of Things)
 - 1.5.5 Sprachassistenten: Vor- und Nachteile
 - 1.5.6 e-Government, digitale Signatur und Handy-Signatur
 - 1.5.7 Schutzmöglichkeiten von Cookie-Tracking und Cookieless-Tracking
 - 1.5.8 Gefahr von Identitätsdiebstahl
 - 1.5.9 Fachbegriff Netzneutralität
 - 1.5.10 Nutzung von biometrischen Daten: Vor- und Nachteile
 - Vorteile der Nutzung von biometrischen Daten
 - Nachteile der Nutzung von biometrischen Daten
 - 1.5.11 Unternehmensrichtlinien für Nutzung von sozialen Netzwerken
 - Verhalten und Kommunikation
 - Vertraulichkeit und professionelles Image
 - Interessenkonflikte und rechtliche Compliance
- 1.6 Datenaustausch
 - 1.6.1 Möglichkeiten des Datenaustausches
 - Kabelgebundene Systeme
 - Kabellose Systeme

1. Allgemeiner Teil - Informationstechnologie

1.1 Ergonomische Gestaltung eines Arbeitsplatzes

1.1.1 Ergonomische Einrichtung eines Bildschirmarbeitsplatzes

Die ergonomische Einrichtung eines Arbeitsplatzes beginnt mit der richtigen Auswahl und Anordnung der Möbel und Geräte:

- **Stuhl:** Ein ergonomischer Bürostuhl ist essentiell. Er sollte **höhenverstellbar** sein und eine gute **Lendenwirbelstütze** bieten. Der Stuhl sollte es ermöglichen, dass die **Füße flach auf dem Boden** stehen können, während die **Knie etwa im rechten Winkel** gebeugt sind.
- **Schreibtisch:** Die Höhe des Schreibtisches sollte so eingestellt werden, dass die **Unterarme parallel zum Boden** sind, wenn Sie auf der Tastatur tippen. Dies verhindert eine Überbeanspruchung der Handgelenke.

1.1.2 Optimaler Aufstellungsort von Bildschirmen (Lichteinfall)

Die Positionierung des Bildschirms ist entscheidend, um Reflexionen und Blendungen zu minimieren, die Augenbelastungen verursachen können:

- **Position:** Der Bildschirm sollte so positioniert werden, dass **Fenster seitlich** davon liegen, nicht direkt davor oder dahinter. Dadurch wird direkter Lichteinfall und Blendung durch Sonnenlicht vermieden.
- **Entfernung und Höhe:** Der Bildschirm sollte etwa **eine Armlänge entfernt** sein. Die **Oberkante** des Bildschirms sollte auf oder **leicht unter Augenhöhe** sein, um den Hals und die Augen zu schonen.

1.1.3 Gesetzliche Bestimmungen von Pausen bei Bildschirmarbeit

In vielen Ländern gibt es gesetzliche Regelungen, die Pausen für Bildschirmarbeiter vorschreiben, um Überanstrengung und Ermüdung der Augen zu vermeiden. In der Regel wird empfohlen:

- **Kurze Pausen** von **5-10 Minuten nach jeweils einer Stunde** kontinuierlicher Bildschirmarbeit.
- **Regelmäßige längere Pausen** und die Möglichkeit, den Arbeitsplatz oder die Arbeitshaltung zu wechseln.

1.1.4 Schutzmaßnahmen und körperliche Entspannungsübungen

Um körperlichen Schäden vorzubeugen, sind regelmäßige Bewegungspausen wichtig.

- **Mikropausen:** Kurze Pausen einlegen, um aufzustehen, sich zu strecken und die Position zu wechseln.
- **Augenübungen:** Regelmäßiges Fokussieren auf entfernte Objekte, um die Augenmuskulatur zu entspannen.
- **Rückenübungen:** Einfache Dehnungsübungen für den Rücken und die Schultern können helfen, Verspannungen zu lösen und die Blutzirkulation zu fördern.

1.2 Arbeitssicherheit und Schutzmaßnahmen

1.2.1 Arbeitssicherheit und Schutzmaßnahmen

Arbeitssicherheit umfasst alle Maßnahmen und Vorkehrungen, die darauf abzielen, **Unfälle am Arbeitsplatz zu verhindern** und die **Gesundheit der Mitarbeiter zu schützen**. Wichtige Schutzmaßnahmen beinhalten:

- Regelmäßige **Schulungen und Unterweisungen** der Mitarbeiter.
- Bereitstellung und Verwendung **persönlicher Schutzausrüstung** (PSA).
- Sicherstellung, dass alle Geräte und Maschinen **regelmäßig gewartet und geprüft** werden.
- Ergonomische Gestaltung des Arbeitsplatzes.

1.2.2 Kenntnisse über Wirkungsweise und Gefahren des elektrischen Stroms

Mensch im Stromkreis

Elektrischer Strom kann **lebensgefährliche Verletzungen** wie **Verbrennungen, elektrische Schocks** und andere **physische Schäden** verursachen. Wichtig ist das Verständnis darüber, dass bereits geringe Stromstärken gefährlich sein können. Sicherheitsmaßnahmen beinhalten:

- **Vermeidung von Kontakt mit spannungsführenden Teilen.**
- Einsatz von **isolierenden Schutzausrüstungen**.
- Sicherstellung, dass die elektrischen Installationen den **geltenden Normen** entsprechen.

In öffentlichen Stromnetzen, bei denen ein Pol geerdet ist, kann der Stromkreis über leitende Objekte wie Wasserleitungen geschlossen werden. Die Stromstärke, die durch den menschlichen Körper fließt, hängt gemäß dem Ohmschen Gesetz von der Spannung und Faktoren ab, die den Körperwiderstand beeinflussen:

- **Berührungsfläche:** Größere Flächen reduzieren den Widerstand.
- **Berührungsdruck:** Starker Druck senkt den Widerstand.
- **Feuchtigkeit:** Nässe verringert den Widerstand.
- **Spannung:** Höhere Spannungen senken den Widerstand.

Der **Körperwiderstand** kann stark variieren und ist schwer vorhersehbar, typischerweise **zwischen einigen hundert Ohm und 10 kΩ**, abhängig von Hautbedingungen und Kontaktfläche.

Bei 230 V Netzspannung können Ströme von einigen Milliampere bis zu einem halben Ampere durch den Körper fließen, wobei die Auswirkungen von Stromstärke, Dauer und Weg des Stroms durch den Körper abhängen.

Bei **Wechselstrom von 50 Hertz** und einer **Einwirkdauer von über einer Sekunde** zeigen sich folgende Effekte bei verschiedenen Stromstärken:

- **ca. 1 mA:** Wahrnehmung und Schmerz beginnen.
- **ca. 15 mA:** Kritische Schwelle; unwillkürliche Muskelkontraktionen können >dazu führen, dass man einen leitenden Gegenstand nicht loslassen kann.

- **ca. 40 mA:** Lebensgefahr durch Kammerflimmern, das zu einer unkoordinierten Herztätigkeit und schnellem Tod durch Sauerstoffmangel im Gehirn führen kann.

Die Vorschriften setzen sichere **Grenzwerte für nicht lebensgefährliche Körperströme** bei **65 V für Wechselstrom und 120 V für Gleichstrom** fest. Kurze Stromstöße unter 0,2 Sekunden werden besser toleriert.

Gesetze und Vorschriften

In Österreich müssen nach dem Elektrotechnikgesetz alle neuen oder wesentlich geänderten elektrischen **Anlagen und Betriebsmittel** den **nationalen (OVE), europäischen (EN) oder internationalen Normen** entsprechen, die gesetzlichen Charakter haben. Hersteller und Verkäufer haften für die Einhaltung dieser Vorschriften. Das **ÖVE-Prüfzeichen**, vergeben von autorisierten Stellen, bestätigt die Übereinstimmung eines Geräts mit diesen Vorschriften.

Elektroschutzkonzept

Ziel: Schutz vor Gefahren durch elektrischen Strom.

Unfallgefahr	Schutzmaßnahme
Direktes Berühren aktiver Leiter (leitende Teile mit Betriebsspannung)	Basisschutz: Schutz gegen direktes Berühren.
Berührungsspannung an inaktiven Teilen durch Isolationsfehler	Fehlerschutz: Schutz bei indirektem Berühren.

Basisschutz: Verhindert direktes Berühren spannungsführender Teile durch Isolierung, Abdeckungen und Montage außerhalb der Reichweite.

Fehlerschutz: Schützt gegen Spannung an Gehäusen und Geräten bei Isolationsfehlern durch Maßnahmen wie Schutzisolierung, Schutz- und Funktionskleinspannung, Schutzerdung, Schutztrennung, Nullung und Fehlerstromschutzschaltungen.

Zusatzschutz: Tritt bei Versagen von Basis- oder Fehlerschutz in Kraft, besonders in gefährlichen Umgebungen, einschließlich Fehlerstromschutzschalter und lokalem Potenzialausgleich.

Schutz gegen direktes Berühren - Basisschutz

Ziel: Schützen von Personen vor elektrischem Strom durch zufällige Berührung aktiver Leiter.

Methoden:

- **Isolierung:** Anwendung von Isoliermaterialien, insbesondere bei Leitungen.
- **Abdeckungen (Gehäuse):** Verhindert Berührung aktiver Teile, wobei Lüftungsschlitze so klein sein müssen, dass kein Kontakt mit spannungsführenden Teilen möglich ist.
- **Montage außer Handbereich:** Platzierung aktiver Leiter so, dass sie nicht erreicht werden können, z.B. bei Freileitungen.

Zusätzliche Schutzmaßnahmen:

- Bei Arbeitsumgebungen mit sperrigen Gegenständen müssen Abstände vergrößert werden.
- **Basisisolierung** muss vor **mechanischer Beschädigung und Überhitzung geschützt** werden und soll den **betriebllichen Belastungen standhalten**.
- Leitungen und **Geräte** müssen **entsprechend der erwarteten Beanspruchung** ausgewählt werden.
- Bewegliche Leitungen benötigen **Zug- und Schubentlastung sowie Knickschutz**.
- Bei Steckverbindungen auf Nennstrom achten und Klemmen fest anziehen.

Sicherheitsregeln für Arbeiten an elektrischen Anlagen:

- **Abschalten:** Allpolig und allseitig.
- **Gegen Wiedereinschalten sichern.**
- **Auf Spannungsfreiheit prüfen.**
- **Erden und Kurzschließen.**
- **Benachbarte spannungsführende Teile abdecken und Gefahrenstellen eingrenzen.**

Schutz bei indirektem Berühren - Fehlerschutz

Hintergrund: Indirektes Berühren tritt auf, wenn bei einem elektrischen Gerät der Schutzklasse 1 ein Körperschluss vorliegt – eine Verbindung zwischen einem aktiven Leiter und dem Gehäuse durch einen Fehler in der Basisisolierung. Dadurch kann das Gehäuse unter Spannung stehen.

Spannungsarten:

- **Fehlervspannung (UF):** Spannung zwischen äußeren leitfähigen Teilen und Bezugserde bei Isolationsfehlern.
- **Berührungsspannung (UT):** Spannung, die am Körper auftritt, wenn dieser von Strom durchflossen wird. Diese Spannung ist potenziell gefährlich und kann unter ungünstigen Umständen so hoch wie die Fehlervspannung sein.

Ursachen für Isolationsfehler:

- Überlastung und hohe Temperaturen.
- Schlechte Behandlung und Alterung des Gerätes.
- Fehlen von Zugentlastung und Knickschutz.
- Einwirkung von Schmutz und Feuchtigkeit, die Kriechströme verursachen.
- Beschädigte Anschlussklemmen.

Risikobereiche: Besonders hoch ist das Risiko im Freien und in feuchten Umgebungen wie Bädern, Werkstätten, Kesselhäusern und Baustellen, wo leicht eine Erdverbindung entstehen kann.

Schutzmaßnahmen:

- **Basisisolierung:** Eine einwandfreie und dauerhafte Isolierung ist essentiell.
- **Errichtung der Anlage:** Sorgfältige Installation und Wartung elektrischer Anlagen zur Minimierung von Risiken.
- **Fehlerschutz:** Notwendige Sicherheitsmaßnahmen für den Fall eines Körperschlusses, besonders bei Geräten und Anlagen mit Nennspannungen über 65 V Wechselstrom und 120 V Gleichstrom gegen Erde, da hier Fehlerschutz gesetzlich vorgeschrieben ist.

Schutzklassen elektrischer Geräte

Schutzklassen elektrischer Geräte

Elektrische Geräte werden in drei Schutzklassen eingeteilt, die angeben, welcher Fehlerschutz vorgesehen ist:

Schutzklasse	Ausführung	Anschlussleitung	Stecker	Beispiele
I	Betriebsisolation, Anschlussklemme für Schutzleiter	Mit Schutzleiter	Schutzkontaktstecker mit Schutzleiter	Waschmaschinen, Elektroherde, Personal Computer
II	Schutzisoliert, doppelte/verstärkte Isolation, keine Schutzleiterklemme	Kein Schutzleiter	Konturen- oder Flachstecker, eventuell Schukostecker	Handwerkzeuge, Küchengeräte, Audio- und Videogeräte
III	Für Kleinspannung bis 50 V, keine Schutzleiterklemme	Kein Schutzleiter	Stecker, die nicht in höhere Spannungssteckdosen passen	Kinderspielzeug, Notebook, Geräte mit externem Netzteil

1.2.3 Kenntnisse über Verhalten und Maßnahmen bei einem Elektrounfall (Reihenfolge)

Rettungsvorgang

Den Verunglückten aus dem Stromkreis befreien:

- Bei Spannungen bis 1000 V den Stecker ziehen oder die Anlage abschalten.
- Isolierte Hilfsmittel nutzen, um den Verunglückten sicher zu bergen.
- Kurzschließen oder Durchtrennen der Leitungen nur erwägen.

Erste Hilfe leisten:

- Überprüfen von Atmung und Bewusstsein.
- Bei Bedarf mit Wiederbelebungsmaßnahmen beginnen.

Notdienste rufen:

- Unverzüglich einen Arzt oder Rettungsdienst alarmieren.

Unfall melden:

- Meldepflicht beachten und den Unfall bei den Behörden melden.

Zusätzliche Sicherheitshinweise:

- Bei Spannungen über 1000 V sollte jede Annäherung vermieden und nur durch Fachpersonal erfolgen.
- Der Retter sollte stets darauf achten, **sich selbst und andere nicht zu gefährden**.

1.2.4 Kenntnisse über Gefahren bei einem Brand und richtiges Verhalten beim Brandfall (Reihenfolge)

Im Brandfall sollte folgendermaßen gehandelt werden:

1. Alarmierung der Feuerwehr.
2. Warnung der anderen Personen im Gebäude.
3. Verlassen des Gebäudes über die gekennzeichneten Notausgänge.
4. Nach Möglichkeit Bekämpfung des Feuers mit geeigneten Feuerlöschmitteln, ohne sich selbst zu gefährden.

1.2.5 Kenntnisse über CO₂- und Pulver-Feuerlöscher

- **CO₂-Feuerlöscher** eignen sich besonders für Brände von flüssigen oder gasförmigen Stoffen und sind effektiv bei elektrischen Bränden, da sie nicht leitend sind.
- **Pulver-Feuerlöscher** sind universell einsetzbar und wirksam gegen Brandklassen A, B und C, allerdings können sie erhebliche Nebenschäden verursachen, besonders bei elektronischen Geräten.

1.2.6 Richtige Verwendung von Feuerlöschern bei elektrischen Anlagen

Bei elektrischen Anlagen sollten vorzugsweise CO₂-Feuerlöscher verwendet werden, da sie den Brand löschen können, ohne weitere Schäden an der Elektronik zu verursachen. Wichtig ist, den Feuerlöscher auf die Basis des Feuers zu richten und ihn in sicherem Abstand zu verwenden.

1.2.7 Richtiger Umgang und korrekte Lagerung von Akkus oder Batterien

- Lagerung in trockenen, kühlen Räumen.
- Vermeidung von Kurzschlüssen, z.B. durch Abdecken der Kontakte.
- Regelmäßige Kontrolle auf Beschädigungen oder Auslaufen.

1.2.8 Kenntnisse über umweltgerechte Entsorgung von Elektronikschrott, Toner, Akkus oder Batterien

- Trennung von normalen Abfällen.
- Rückgabe an spezialisierte Sammelstellen oder Händler.
- Beachtung der spezifischen Entsorgungsvorschriften für gefährliche Stoffe.

1.2.9 Kenntnisse über arbeitsrechtliche Gesetze (KJBG, ASchG, GIBG)

1. **Kinder- und Jugendlichen-Beschäftigungsgesetz (KJBG):** Das KJBG regelt die Arbeitsbedingungen für Kinder und Jugendliche in Österreich. Es zielt darauf ab, die Sicherheit, Gesundheit und Entwicklung junger Menschen am Arbeitsplatz zu schützen. Das Gesetz definiert, wer als Kind oder Jugendlicher gilt, legt fest, welche Arten von Arbeit erlaubt oder verboten sind, und regelt Arbeitszeiten, Ruhezeiten sowie die erforderlichen Pausen. Zum Beispiel dürfen Kinder unter 15 Jahren grundsätzlich nicht beschäftigt werden, außer in leichten und für Kinder geeigneten Tätigkeiten.

2. **ArbeitnehmerInnenschutzgesetz (ASchG):** Das ASchG umfasst Vorschriften zur Sicherstellung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmerinnen und Arbeitnehmer am

Arbeitsplatz. Das Gesetz enthält Regelungen zu den Pflichten des Arbeitgebers, wie zum Beispiel die Durchführung von Gefährdungsbeurteilungen, die Bereitstellung von Sicherheitsausrüstungen und die Sicherstellung einer angemessenen Ausbildung der Mitarbeiter in Bezug auf Sicherheitspraktiken. Darüber hinaus regelt es auch die Rechte und Pflichten der ArbeitnehmerInnen, einschließlich der Meldung von Sicherheitsmängeln.

3. **Gleichbehandlungsgesetz (GlBG):** Das GlBG dient dem Schutz vor Diskriminierung in der Arbeitswelt aufgrund von Geschlecht, Alter, sexueller Orientierung, Religion, Weltanschauung oder ethnischer Zugehörigkeit. Es regelt die Gleichbehandlung in arbeitsrechtlichen Angelegenheiten, einschließlich Einstellung, Arbeitsbedingungen, Aufstiegschancen, Entgeltgleichheit und den Schutz vor Belästigung am Arbeitsplatz. Das Gesetz sieht auch spezifische Maßnahmen und rechtliche Schritte vor, die Betroffene im Falle einer Diskriminierung ergreifen können.

1.3 Technische Dokumentation

1.3.1 Aufgabe und Strukturierung von Testläufen

Testläufe dienen dazu, die Funktionalität und Stabilität von Software oder Systemen unter kontrollierten Bedingungen zu überprüfen. Die Strukturierung erfolgt oft in Phasen wie Planung, Durchführung und Analyse:

- **Planung:** Festlegen von Testzielen, Testfällen und Erfolgskriterien.
- **Durchführung:** Ausführen der Tests, oft unter Verwendung spezifischer Testsoftware.
- **Analyse:** Auswerten der Ergebnisse und Dokumentieren von Abweichungen oder Fehlern.

1.3.2 Inhalt einer technischen Dokumentation/eines technischen Protokolls

Eine technische Dokumentation enthält in der Regel:

- **Zielsetzung** des Projekts oder der Arbeit.
- **Methodik** oder Verfahrensanweisungen.
- **Ergebnisse** und deren Interpretation.
- **Fehler- und Problemmeldungen** sowie Lösungsansätze.

1.3.3 Aufbereitung einer technischen Dokumentation/eines technischen Protokolls

Die Aufbereitung sollte klar, präzise und systematisch erfolgen. Verwendung von Abschnitten, Überschriften und Listen hilft, Informationen leicht zugänglich zu machen. Grafiken und Tabellen können zur Visualisierung von Daten beitragen.

1.3.4 Anwendung der Schrittaufzeichnung/Step Recorder

Der Step Recorder in Windows ist ein Tool zur Aufzeichnung von Schritten, die ein Benutzer auf seinem Computer ausführt. Es ist hilfreich für die Fehlerdiagnose oder die Erstellung von Trainingsmaterial.

1.3.5 Beilagen technischer Dokumentationen (Testprotokoll, Netzwerkplan, ...)

Beilagen wie Testprotokolle oder Netzwerkpläne ergänzen die Hauptdokumentation und bieten detaillierte Einblicke in spezifische Aspekte der Arbeit.

1.3.6 Gestaltung und Vorbereitung von Präsentationen

Für die Präsentation technischer Inhalte sollte auf klare Struktur, Verständlichkeit und visuelle Unterstützung durch Diagramme, Charts und Bilder geachtet werden. Tools wie Microsoft PowerPoint oder Google Slides sind hierfür geeignet.

1.4 Datenschutzgrundverordnung (DSGVO)

1.4.1 Aktuelle DSGVO

Die Datenschutzgrundverordnung ist ein Regelwerk der EU, das den Schutz personenbezogener Daten innerhalb der Europäischen Union regelt. Es zielt darauf ab, die Privatsphäre der Bürger zu schützen und die Datenverarbeitung durch Unternehmen und öffentliche Stellen zu regulieren.

1.4.2 Datenminimierung

Der Grundsatz der Datenminimierung besagt, dass nur so viele personenbezogene Daten erhoben und verarbeitet werden dürfen, wie unbedingt notwendig für den festgelegten Zweck.

1.4.3 Fachbegriffe laut DSGVO

- **Betroffene Personen:** Individuen, deren personenbezogene Daten verarbeitet werden.
- **Verantwortlicher:** Die Person oder Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- **Auftragsverarbeiter:** Eine Person oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.4.4 Rechte von betroffenen Personen

Dazu gehören das Recht auf Auskunft, Berichtigung, Löschung („Recht auf Vergessenwerden“), Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch gegen die Verarbeitung.

1.4.5 Personenbezogene und sensible Daten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Sensible Daten umfassen Daten über rassische oder ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben.

1.4.6 Kopplungsverbot

Das Kopplungsverbot besagt, dass die Erbringung einer Dienstleistung nicht davon abhängig gemacht werden darf, dass die betroffene Person der Verarbeitung mehr personenbezogener Daten zustimmt, als für die Erbringung der Dienstleistung notwendig ist.

1.4.7 Datenschutzbeauftragter

Ein Datenschutzbeauftragter überwacht die Einhaltung der DSGVO innerhalb einer Organisation. Er ist Ansprechpartner für Datenschutzfragen sowohl intern als auch für Aufsichtsbehörden und betroffene Personen.

1.4.8 Pflichten bei Datendiebstahl

Unternehmen sind verpflichtet, Datenschutzverletzungen innerhalb von 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde zu melden. Betroffene Personen müssen ebenfalls informiert werden, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht.

1.4.9 Weitere rechtliche Grundlagen

- **Urheberrecht:** Schützt die Rechte von Kreativen und Urhebern an ihren Werken. Der Gültigkeitsbereich umfasst Werke wie Literatur, Musik, Kunst und Software.
- **Gewährleistung und Garantie:** Gewährleistung ist gesetzlich vorgeschrieben und deckt Mängel ab, die bereits zum Zeitpunkt des Kaufs bestanden. Garantie ist eine freiwillige Zusicherung des Herstellers und kann über die Gewährleistung hinausgehen.
- **E-Commerce-Gesetz (ECG):** Regelt die rechtlichen Rahmenbedingungen für elektronische Geschäfte, insbesondere Online-Handel.
- **Telekommunikationsgesetz (TKG):** Regelt die Telekommunikationsdienste und -netze, Datenschutz und den Wettbewerb im Telekommunikationssektor.
- **Pflichtangaben eines Homepage-Betreibers (Impressum):** Informationen wie Name des Unternehmens, Kontaktdaten, Registrierungsnummer, Umsatzsteuer-ID müssen klar erkennbar sein.
- **Pflichtangaben beim E-Mail-Verkehr von Unternehmen:** Ähnlich wie im Impressum müssen E-Mails von Unternehmen vollständige Kontaktdaten und Firmeninformationen enthalten.
- **Gesetzliche Einhaltung von Bildschirmspausen:** Bestimmungen zu Pausen bei Bildschirmarbeit sind wichtig für die Gesundheit der Arbeitnehmer und in verschiedenen nationalen Arbeitsgesetzen festgelegt.

1.5 Fachbegriffe und Grundlagen in der Informationstechnik

1.5.1 Fachbegriff Big Data

Definition: Big Data bezieht sich auf extrem große Datenmengen, die aus verschiedenen Quellen stammen und mit herkömmlichen Datenverarbeitungsmethoden nicht analysiert werden können.

Anwendung: Big Data wird genutzt, um Muster und Trends zu erkennen, insbesondere in Bereichen wie Marketing, Gesundheitswesen, Finanzen und beim Internet der Dinge (IoT).

1.5.2 Fachbegriff Web 2.0

Definition: Web 2.0 beschreibt die zweite Generation des Internets, die durch interaktive und kollaborative Elemente gekennzeichnet ist, im Gegensatz zu den statischen Seiten des früheren Web 1.0.

Beispiele: Soziale Netzwerke, Blogs, Wikis und interaktive Kommentarsektionen.

1.5.3 Fachbegriff Industrie 4.0

Definition: Industrie 4.0 bezieht sich auf die vierte industrielle Revolution, die durch Automatisierung, Datenvernetzung und künstliche Intelligenz in der Fertigungstechnik gekennzeichnet ist.

Technologien: Robotik, künstliche Intelligenz, IoT, und cyber-physische Systeme.

1.5.4 Fachbegriff IoT (Internet of Things)

Definition: IoT steht für das "Internet der Dinge", also die Vernetzung von physischen Objekten mit dem Internet, die dann Daten sammeln und austauschen können.

Anwendung: Smart Homes, intelligente Verkehrssteuerung, Gesundheitsüberwachung.

1.5.5 Sprachassistenten: Vor- und Nachteile

Vorteile:

- Erhöhte Produktivität durch Sprachbefehle.
- Einfacher Zugriff auf Informationen und Gerätesteuerung.

Nachteile:

- Datenschutzbedenken bei gesammelten Sprachdaten.
- Risiko von Fehlinterpretationen und Fehlfunktionen.

1.5.6 e-Government, digitale Signatur und Handy-Signatur

e-Government: Nutzung von digitalen Technologien zur Erbringung öffentlicher Dienstleistungen.

Digitale Signatur: Verschlüsselte elektronische Unterschrift, die die Identität des Unterzeichners bestätigt und die Integrität der signierten Daten sichert.

Handy-Signatur: Eine Form der digitalen Signatur, die über ein Mobilgerät generiert wird und rechtlich bindend ist.

1.5.7 Schutzmöglichkeiten von Cookie-Tracking und Cookieless-Tracking

Cookie-Tracking: Nutzer können Cookies in ihren Browser-Einstellungen verwalten und blockieren.

Cookieless-Tracking: Schwieriger zu kontrollieren, da es auf Techniken wie Fingerprinting basiert. Nutzer können Datenschutztools wie VPNs und Anti-Tracking-Software verwenden.

1.5.8 Gefahr von Identitätsdiebstahl

Risiken: Missbrauch persönlicher Daten zur Eröffnung von Konten, Durchführung von Transaktionen oder zur Erlangung von Leistungen.

Prävention: Sichere Passwörter, regelmäßige Überprüfung von Kontoberichten, und Vorsicht bei der Preisgabe persönlicher Informationen.

1.5.9 Fachbegriff Netzneutralität

Definition: Netzneutralität ist das Prinzip, dass Internetdienstanbieter alle Daten im Internet gleich behandeln und keinen Verkehr diskriminieren oder bevorzugen dürfen.

1.5.10 Nutzung von biometrischen Daten: Vor- und Nachteile

Diese Daten umfassen persönliche Merkmale wie Fingerabdrücke, Gesichtserkennung, Iriserkennung und sogar Stimmerkennung, die zur Identifikation und Authentifizierung in verschiedenen Sicherheitssystemen verwendet werden.

Vorteile der Nutzung von biometrischen Daten

Hohe Sicherheit: Biometrische Merkmale sind in der Regel einzigartig für jede Person. Diese Einzigartigkeit bietet eine hohe Sicherheitsstufe, da die Wahrscheinlichkeit, dass zwei Personen exakt die gleichen biometrischen Daten haben, extrem gering ist. Im Vergleich zu traditionellen Sicherheitsmaßnahmen wie Passwörtern, die gehackt oder vergessen werden können, bieten biometrische Systeme eine robustere Lösung.

Schneller und bequemer Zugriff: Biometrische Systeme ermöglichen einen schnellen und bequemen Zugang zu Geräten und Diensten. Anstatt sich lange Passwörter zu merken oder Sicherheitsfragen zu beantworten, können Benutzer durch einen einfachen Scan ihres Fingerabdrucks oder durch Gesichtserkennung auf ihre Geräte und persönlichen Konten zugreifen. Diese Methoden sind nicht nur schneller, sondern auch benutzerfreundlicher, was sie besonders attraktiv für den alltäglichen Gebrauch macht.

Nachteile der Nutzung von biometrischen Daten

Datenschutzrisiken: Obwohl biometrische Daten eine hohe Sicherheit bieten, bergen sie auch Risiken im Hinblick auf den Datenschutz. Wenn biometrische Daten kompromittiert oder gestohlen werden, können die Konsequenzen gravierend sein. Im Gegensatz zu einem Passwort, das zurückgesetzt

werden kann, sind biometrische Daten dauerhaft mit einer Person verbunden und können nicht einfach geändert werden. Dies stellt ein signifikantes Risiko dar, falls die Daten in die falschen Hände gelangen.

Fehlerraten bei der Erkennung: Biometrische Systeme sind nicht fehlerfrei und können unter bestimmten Umständen zu Fehlern bei der Erkennung führen. Falsche Ablehnungen (False Rejection Rate, FRR) treten auf, wenn ein authentischer Benutzer fälschlicherweise nicht erkannt wird, während falsche Annahmen (False Acceptance Rate, FAR) auftreten, wenn das System eine nicht autorisierte Person irrtümlich akzeptiert. Diese Fehlerraten können die Zuverlässigkeit biometrischer Systeme beeinträchtigen und stellen eine Herausforderung für ihre breite Akzeptanz dar.

1.5.11 Unternehmensrichtlinien für Nutzung von sozialen Netzwerken

Verhalten und Kommunikation

- **Inhaltsrichtlinien:** Klare Definitionen erlaubter Inhalte, um Datenschutz und Professionalität zu wahren.
- **Verhaltenskodex:** Vorgaben für professionelle und respektvolle Kommunikation.
- **Schulung:** Mitarbeiter werden regelmäßig in sicheren und effektiven Umgang mit sozialen Medien trainiert.

Vertraulichkeit und professionelles Image

- **Datenschutz:** Richtlinien betonen den Schutz personenbezogener Daten.
- **Imagepflege:** Anweisungen zum professionellen Umgang mit öffentlichem Feedback und zur Imagepflege.
- **Verantwortlichkeiten:** Festlegung, wer für Unternehmensposts verantwortlich ist und Prüfverfahren vor der Veröffentlichung.

Interessenkonflikte und rechtliche Compliance

- **Offenlegung:** Mitarbeiter müssen potenzielle Interessenkonflikte offenlegen.
- **Rechtliche Einhaltung:** Posts müssen alle gesetzlichen Anforderungen erfüllen, inklusive Werbevorschriften und Urheberrechte.
- **Überwachung:** Kontinuierliche Überwachung der Einhaltung der Richtlinien und Maßnahmen bei Nichteinhaltung.

1.6 Datenaustausch

1.6.1 Möglichkeiten des Datenaustausches

Kabelgebundene Systeme

- **Kupferkabel:** Diese umfassen Twisted-Pair-Kabel, die für die meisten Netzerkwendungen verwendet werden, und Koaxialkabel, die häufig für Breitbandnetzwerke verwendet werden.
- **Lichtwellenleiter (Glasfaser):** Diese bieten höhere Übertragungsgeschwindigkeiten und -reichweiten mit geringerer Störanfälligkeit. Sie sind ideal für Netzwerke, die hohe Bandbreiten erfordern.

Kabellose Systeme

- **WLAN (Wireless Local Area Network):** Ermöglicht die kabellose Vernetzung von Geräten innerhalb eines begrenzten Bereichs.
- **Mobilfunktechnologien** (z.B. GSM, UMTS, LTE): Ermöglichen die Datenübertragung über größere Entfernungen und sind weit verbreitet für den mobilen Internetzugang.
- **Infrarot- und Bluetooth-Technologien:** Meist für kurze Distanzen und spezifische Anwendungen wie die Verbindung von Peripheriegeräten verwendet.