Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2022:

Einführung in den Datenschutz (3)
& OTT-Dienste

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung I

Aufgabe:

- Für ein **Pandemie-Web-Portal** wurde Folgendes geplant:
  - Das Web-Portal soll auf Gesundheitsdaten aus der Pandemie-Datenbank lesend zugreifen können, wobei nur die Betroffenen unmittelbar ihre eigenen personenbezogenen Daten und alle anderen Stellen nur pseudonymisierte Gesundheitsdaten sowie weitere Daten sehen, die jeweils hinzugespeichert worden sind
  - Die Betroffenen, welche in der Pandemie-Datenbank erfasst sind, sollen eine fortlaufende Nummer als Benutzerkennung erhalten und das Web-Portal nach Eingabe eines frei gewählten Passwortes nutzen können, um ergänzende Angaben zu relevanten Begleitumstände selbst eingeben zu können
  - Betroffene sollen ihre Eingaben nach Eintragung per Mail erhalten
  - Im Web-Portal sollen die Betroffenen sehen können, wie Rahmenbedingungen (begünstigende und beeinträchtigende Faktoren), Impfentwicklungen und Krankheitsverläufe bei anhand vordefinierter Kriterien als vergleichbar geltenden Patienten ausgesehen haben
  - Das Web-Portal soll als Public Cloud implementiert werden

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung II

Aufgabe: (Fortsetzung)

- Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Datenschutz-Folgenabschätzung (gem. Art. 35 EU-DSGVO) sehen (unter Berücksichtigung der Bußgeldbestimmungen und Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten), schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß nächstehender 3x3-**Risk-Map**. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (1)

1) Ermittlung potenzieller Datenschutzrisiken:

- Lesender Zugriff auf eigene Daten im Web-Portal auf Pandemiedaten
  1. Pandemiedaten offensichtlich auf Betroffene zuordnenbar → Gefahr: Unbefugte Offenlegung ggf. möglich (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Benutzerkennung via fortlaufender Nummer & freie Passwortwahl
  2. Enumerative Zugangsdaten → Gefahr: kein unmittelbarer Schaden
  3. Mangelnder Zugriffsschutz bei geringer Passwortgüte → Gefahr: Unbefugter Zugang (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)
- Bestätigungsmail für durchgeführte Eingaben
  4. Mail-Server mit Web-Portal direkt verbunden → Gefahr: kein unmittelbarer Schaden (unbeachtlich des Schutzbedarfs für den Inhalt der Eingaben…)
- Einsicht in Vergleichsdaten via Web-Portal
  5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil → Gefahr: Profiling (formaler Verstoß, da durch diese DSFA ja behandelt)

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (2)

1) Ermittlung potenzieller Datenschutzrisiken: (Fortsetzung)

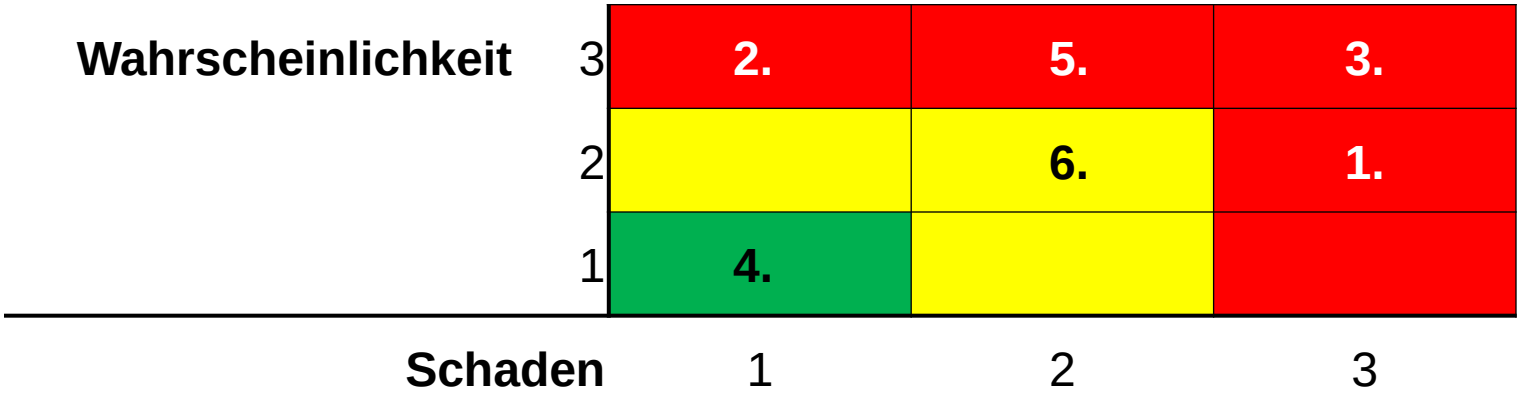
- Web-Portal als Public Cloud implementiert
  6. Pandemiedaten unzureichend geschützt → Gefahr: Unbefugte Offenlegung ggf. möglich (Art. 32 Abs. 2 EU-DSGVO → Bußgeld nach Art. 83 Abs. 4 lit. a EU-DSGVO)

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (3)

2) Abschätzung der Eintrittsstufe:

1. Zuordnenbare Pandemiedaten: Gefahreintritt wahrscheinlich, da Angreifer nur über begrenzte Fähigkeiten & Ressourcen verfügen muss, um Daten z.B. via SQL-Injection abrufen zu können, da Daten ja durch den Nutzer eigegeben werden können
2. Enumerative Zugangsdaten: Gefahreintritt sicher, da entsprechendes Ausprobieren voraussetzungslos möglich ist
3. Mangelnder Zugriffsschutz bei geringer Passwortgüte: Gefahreintritt sicher, da Passwort-Cracker leicht downloadbar sind & schlechte Passwörter i.d.R. bereits leicht zum Erfolg führen (z.B. Benutzerkennung = Passwort)
4. Mail-Server mit Web-Portal direkt verbunden: Gefahreintritt nur möglich, da Angreifer erst noch den Verbindungspfad ermitteln muss
5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil: Gefahreintritt sicher, aufgrund der Voraussetzungen aus 2. & 3.
6. Implementation via Public Cloud: Gefahreintritt wahrscheinlich, da i.d.R. preisgünstig aufgrund geringerer Schutzvorkehrungen

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (4)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

Wahrscheinlichkeit: **Eintritt einer Verletzung des Schutzes personenbezogener Daten**	**Schaden:** **Grad der Verletzung des Schutzes personenbezogener Daten**
1 = möglich	1 = niedrig (ohne unmittelbare Wirkung)
2 = wahrscheinlich	2 = mittel (formaler Verstoß)
3 = sicher	3 = hoch (Bußgeld/Meldepflicht)

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (5)

3) Handlungsempfehlung:

1. Unbeschränkter Zugriff auf alle personenbezogene Pandemie-Daten
   → Datenvalidierung sicherstellen (SQL-Injection verhindert) & Zuordnungsdaten mittels Broker schützen
2. Enumerative Zugangsdaten
   → Benutzerkennung frei wählen lassen
3. Mangelnder Zugriffsschutz bei geringer Passwortgüte
   → Mindestvorgaben für Passwortgüte festlegen (Komplexität, Länge)
4. Mail-Server mit Web-Portal direkt verbunden
   → akzeptierbar, wenn Verbindungspfad nicht ermittelbar ist und ein Angreifer nicht als Man-in-the-Middle zwischenschalten kann
5. Unbefugter Zugriff ermöglicht Persönlichkeitsprofil
   → nach Änderung zu 2. & 3. ggf. akzeptierbar

3.1 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (6)

3) Handlungsempfehlung: (Fortsetzung)

6. Web-Portal mit Pandemiedaten als Public Cloud
   → Einsatz einer Private Cloud, um Schutzvorkehrungen angemessen für Gesundheitsdaten treffen zu können (oder Auswahl einer Public Cloud, die entsprechende Garantien zusichert)

Anmerkung:

- *Die Angabe der Punkte aus Art. 35 Abs. 7 EU-DSGVO ist bei der Durchführung von Datenschutz-Folgenabschätzungen verpflichtend*
  ° auf systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
  in der Aufgabe jedoch verzichtet, da nach Aufgabenstellung nicht zwingend verlangt

3.2 Datenschutzerklärung

Aufgabe:

- Die Lehrveranstaltung einer Universität soll infolge der Pandemie auf reine Online-Lehre umgestellt werden. Hierzu soll sowohl zur Vorlesung als auch zur Übung eine Lösung zum **Videokonferencing** mit einer Zugangsbeschränkung eingesetzt werden. Entwerfen Sie eine zugehörige **Datenschutzerklärung** zu dessen Einsatz im Sinne von Art. 13 EU-DSGVO!

3.2 Datenschutzerklärung (1)

- Zur Online-Lehre an der Universität werden Vorlesungen und Übungen mittels Videokonferencing abgewickelt, welches vom <<Anbieter>> auf der Grundlage einer Datenschutzvereinbarung unter Einsatz eines Data Centers auf dem Gebiet der EU betrieben wird. Details zur Datenverarbeitung durch dieses Videokonferencing kann der zugehörigen Datenschutzerklärung auf <<Anbieter-Webseite>> entnommen werden.
- Dieses Videokonferencing ist bereits durch Aufruf eines zugesandten Links im Browser nutzbar. Alternativ kann lokal auch eine entsprechende App installiert werden. In beiden Fällen ist ein Aufruf der Webseite des Anbieters bzw. der Universität zumindest initial erforderlich.
- Die Online-Lehre wird unter Ausnutzung einer Zugangsbeschränkung durchgeführt, weshalb die entsprechenden Links stets der Eingabe der lehrveranstaltungsspezifischen Meeting-ID und des zugehörigen Kenncodes bedarf, die vom Organisator der betreffenden Lehrveranstaltung zur Verfügung gestellt wird.

3.2 Datenschutzerklärung (2)

- Bei Nutzung des Videokonferencing werden gespeichert:
  - Angaben zum Benutzer, bestehend aus IP-Adresse, Verbindungsbeginn und -ende, bei Beginn der Veranstaltung selbst eingegebene Nutzerkennung
  - Meeting-Metadaten: Thema, Beschreibung (optional), Teilnehmer IP-Adressen, Geräte-/ Hardware-Informationen
  - Bei Einwahl mit dem Telefon: Angabe zur eingehenden und ausgehenden Rufnummer, Ländername, Start- und Endzeit
  - Bei Eingabe von Chatnachrichten, dem Upload von Dateien oder dem Teilen von Bildschirminhalten: Entsprechende Angaben, die vom Benutzer selbst hierzu ausdrücklich preisgegeben werden
  - Bei Aktivieren des Mikrofons: Tondaten, die vom genutzten Mikrofon seitens des Benutzers aufgezeichnet werden
  - Bei Aktivieren der Kamera: Bilddaten, die von der genutzten Kamera seitens des Benutzers aufgezeichnet werden
- Die mittels Videokonferencing abgewickelte Online-Lehre wird defaultmäßig nicht und ansonsten nur mit Zustimmung aller Beteiligten aufgezeichnet.

3.2 Datenschutzerklärung (3)

- Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Videokonferencing zur universitären Online-Lehre ist Art. 6 Abs. 1 lit. e EU-DSGVO.
- Nach Abschluss der jeweiligen Lehrveranstaltungssessions werden die jeweils gespeicherten Daten automatisch gelöscht. Alle weiteren Speicherdauern richten sich ansonsten nach den Vorgaben für Nutzungsdaten interpersoneller Telekommunikationsdienste im Sinne von § 2 Abs. 2 Nr. 3 TTDSG und zugehörigen Verkehrsdaten.
  *Hinweis: Nach den **§§ 6 Abs. 2, 9 Abs. 2, 12 und 19 TTDSG** resultieren daraus **besondere Schutzvorkehrungen**.*
- Die Teilnehmenden einer Lehrveranstaltung, die mittels Videokonferencing abgewickelt wird, sind dazu aufgerufen, im Rahmen der jeweiligen Sessions nur erforderliche Daten preiszugeben. Das betrifft ausdrücklich auch den gewählten Bildausschnitt (evtl. unter Ausnutzung von Blurring), vorgeführte Bildschirminhalte und die übertragenen Hintergrundgeräusche während das eigene Mikrofon aktiviert ist.
- Alle weiteren Details zu den Betroffenenrechten und den Angaben zum Verantwortlichen kann der **allgemeinen Datenschutzerklärung der Universität** entnommen werden.

3.3 Löschkonzept

Aufgabe:

- Entwerfen Sie unter Beachtung relevanter Vorschriften aus dem TTDSG ein **Löschungskonzept** für eine **Mailingliste**, zu der sich Abonnenten frei eintragen können und die über ein Archiv zugesandter Mails verfügt, welches für alle Abonnenten nach Eingabe frei gewählter Zugangsdaten zugänglich ist! Berücksichtigen Sie dabei auch, wie mit Datensicherungen umzugehen ist.

3.3 Löschkonzept (1)

- Mailingliste ist ein interpersoneller Telekommunikationsdienst
  → Neben den allgemeinen Datenschutzvorschriften aus der EU-DSGVO treten insoweit Vorschriften aus dem TTDSG hinzu
  (aktueller Hinweis: Auf EU-Ebene steht derzeit noch eine Verabschiedung der ePrivacy-Verordnung vor dem Abschluss)
- Die Speicherbegrenzung aus Art. 5 Abs. 1 lit. e EU-DSGVO bezieht sich auf Identifizierungsdaten
- Nach Art. 17 Abs. 1 lit. a EU-DSGVO sind personenbezogene Daten zu löschen, wenn sie für die festgelegten Zwecke nicht mehr notwendig sind
- Nach Art. 30 Abs. 1 lit. f EU-DSGVO sind im Verzeichnis von Verarbeitungstätigkeiten die Regellöschungsfristen festzuhalten
- Daten über Abonnenten sind Bestandsdaten (§ 2 Abs. 2 Nr. 2 TTDSG), Archivdaten Nutzungsdaten (§ 2 Abs. 2 Nr. 3 TTDSG) & das Archiv ein Dienst mit Zusatznutzen (§ 2 Abs. 2 Nr. 5 TTDSG)

3.3 Löschkonzept (2)

- Für Löschungskonzept ist vor allem der Umgang mit dem Mailinglisten-Archiv zu regeln, welches durch die jeweils aktuellen Abonnenten unter Eingabe frei gewählter Zugangsdaten einsehbar ist.
- Das Mailinglisten-Archiv besteht jedoch unabhängig (!) von dem individuellen Abonnement des einzelnen Mitglieds der Mailingliste!
  → Zugehörige Datenschutzerklärung muss ausdrücklich definieren, wie mit entsprechenden Beiträgen ausgeschiedener Abonnenten umgegangen wird; hierbei kann unterschieden werden zwischen den aufrufbaren Header-Daten (welche z.B. mittels Pseudonymisierung vom unmittelbaren Personenbezug befreit werden können) und den Inhalts-Daten, die jedoch nur schwer von spezifischen Angaben befreit werden können, zumal sich weitere Antworten ja mit Zitierung entsprechender Bestandteile kaum noch entsprechend zuordnen lassen!

3.3 Löschkonzept (3)

- In der Einwilligungserklärung zum Abonnement der Mailingliste muss daher die Speicherung gesendeter Beiträge (= Verkehrsdaten mit Zusatznutzen!) und deren Ablage im Mailinglisten-Archiv von der abonnementsbezogenen Löschung im Sinne von § 9 Abs. 2 TTDSG ausdrücklich ausgenommen werden!
- Zum Ausgleich muss aber die Möglichkeit für Abonnenten bestehen, Beiträge, in denen diese ohne ihre Zustimmung bzw. ohne Referenz auf selbst eingestellte Beiträge genannt werden, auf Anforderung löschen zu lassen → Teil des Löschkonzepts
- Die EU-DSGVO bestimmt jedoch nicht exakt, was unter „Löschen“ zu verstehen ist; nach ErwG 39 muss sichergestellt sein, dass Unbefugte keinen Zugang zu den Daten haben und diese Daten auch nicht nutzen können
  → reiner Leserechteentzug nicht ausreichend
  → Pseudonymisierung dagegen u.U. schon, Anonymisierung stellt nach § 9 Abs. 2 TTDSG zulässige Umsetzung dar

3.3 Löschkonzept (4)

- Im Rahmen der Datenschutzerklärung ist folglich festzulegen, ab wann ein Thread, der aus den zu dem betreffenden Thema über die Mailingliste gesandten Beiträgen besteht, aus dem Mailinglisten-Archiv automatisiert gelöscht wird, z.B. nach 6 Jahren (analog zur Aufbewahrungspflicht für Geschäftsbriefe) nach letztem Beitrag in einem betreffenden Thread (i.d.R. wird für ein Mailinglisten-Archiv auch eine kürzere Frist, z.B. 3 Jahre analog zu üblichen Zertifizierungsfristen, ausreichend sein)
  → im Löschkonzept ist entsprechend auszuführen, wie die automatisierte Löschung dann erfolgt
- Nach § 6 Abs. 2 TTDSG muss ein unbefugtes Offenbaren von Nachrichteninhalten nach Stand der Technik vermieden werden
- Aufgrund von § 19 Abs. 2 TTDSG ist in der Datenschutzerklärung über die Möglichkeit zur anonymen oder pseudonymen Nutzung hinzuweisen (→ Löschung von Identifikationsdaten aus Bestandsdaten für Archiv-Nutzer im Löschkonzept auszuführen)

3.3 Löschkonzept (5)

- Nach § 9 Abs. 1 TTDSG sind Nutzungsdaten zum Abruf von Archivdaten unverzüglich zu löschen → Teil des Löschkonzepts
- Mailinglisten-Archivierung setzt jedoch Datensicherung voraus
- Datensicherung = Maßnahme im Sinne von Art. 32 Abs. 1 lit. b und c EU-DSGVO i.V.m. Art. 6 Abs. 1 lit. f EU-DSGVO
- Für Datensicherungen gelten die Fristen des Hauptverfahrens analog, doch müssen Daten nicht gesondert von Datensicherungsmedien entfernt werden (aus technischen Gründen auch schwerlich möglich); hier bestimmt sich die Aufbewahrungsfrist nach der längstbenötigten Frist des Mediums, wobei diese allerdings nicht künstlich erhöht werden darf, indem unnötig Daten hinzugespeichert werden, die eine deutlich längere Aufbewahrungsfrist benötigen (würde sonst dem Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a EU-DSGVO und andererseits der Datenminimierung nach Art. 5 Abs. 1 lit. c EU-DSGVO widersprechen)

3.3 Löschkonzept (6)

- Nach § 35 Abs. 1 BDSG 2018 ist (auf Basis von Art. 23 Abs. 1 lit. j EU-DSGVO) für eine Datensicherung die Einschränkung (= Sperrung) der Datensicherungsdaten ausreichend, da hierfür (im Gegensatz zu den Archivdaten) das Interesse des Betroffenen an der Löschung von vorneherein als gering anzusehen ist und eine Löschung wegen der besonderen Art der Speicherung nur mit unverhältnismäßig hohem Aufwand möglich wäre (sequentielles Umkopieren auf ein anderes Datensicherungsmedium mit dem zusätzlichen Risiko, dass durch Umkopieren ggf. die weiter aufzubewahrenden Daten nicht mehr lesbar sind)

3.4 Einwilligung in Web-Tracking I

Aufgabe:

- Ein Unternehmen möchte die Nutzung ihrer Webseite mittels eines Tracking-Tools analysieren, das die IP-Adressen der Nutzer und die getätigten Klicks sowie die eingegebenen Suchanfragen zu Analysezwecken an einen für derartige Analysen spezialisierten Dritten in einem Drittland ohne angemessenes Datenschutzniveau überträgt. Zu diesem Zweck soll auf dem Endgerät des Nutzers ein Cookie gespeichert werden. Der bereitgestellte Telemediendienst soll eine pseudonyme Nutzung ermöglichen. Formulieren Sie eine geeignete **elektronische Einwilligungserklärung** zur Speicherung des zugehörigen Cookies!

3.4 Einwilligung in Web-Tracking II

Aufgabe:

- *<u>Hinweis:</u>*
  Ziel von Tracking Tools ist die bedarfsgerechte Gestaltung angebotener Telemedien. Das Endgerät wird im TTDSG Endeinrichtung genannt. Das Setzen des Cookies ist nicht erforderlich, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.
- *Gehen Sie in Ihrer Antwort davon aus, dass IP-Adressen als personenbezogenes Datum anzusehen sind, selbst wenn diese dynamisch erzeugt werden.*

3.4 Einwilligung in Web-Tracking (1)

- *IP-Adressen werden nach herrschender Meinung als personenbezogene Daten angesehen, da Online-Kennung (siehe ErwG 30 und das Beispiel 15 zu dynamischen IP-Adressen in WP 136 der EU-Datenschutzgruppe nach Art. 29 EU-DSRL (Vorläufer des Europäischen Datenschutzausschusses)*
- *Aufgabe von Tracking-Tools ist es, das Verhalten der Web-Seiten-Nutzer hinsichtlich deren Klicks und Eingaben auf den bereitgestellten Web-Seiten zu analysieren und daraus Rückschlüsse zur Verbesserung des eigenen Web-Auftritts bzw. der dort angebotenen Produkte / Leistungen ziehen zu können*
  - *→ Ziel: bedarfsgerechte Gestaltung angebotener OTT-Dienste!*
  - *→ Einwilligung nach § 9 Abs. 2 TTDSG nötig!*
  - *→ Wegen Datenübertragung in Drittland Art. 49 Abs.1 lit. a EU-DSGVO bei Einwilligung berücksichtigen!*
  - *→ Da Cookie auf Endeinrichtung des Nutzers gespeichert wird, muss Einwilligung zudem § 25 Abs. 1 TTDSG erfüllen!*
  - *→* ***Cookie darf erst nach Einwilligung gesetzt werden****!*

3.4 Einwilligung in Web-Tracking (2)

Hiermit willige ich ein, dass die gespeicherte IP-Adresse, meine Klicks sowie von mir eingegebene Suchanfragen zum Zweck der bedarfsgerechten Gestaltung der Webseite von der <Bezeichnung des Verantwortlichen> unter Berücksichtigung der zugesicherten pseudonymen Nutzung verwendet werden dürfen. Ich bin damit einverstanden, dass die Analysen durch einen spezialisierten Dritten in einem Drittland ohne angemessenes Datenschutzniveau durchgeführt werden. Ich wurde darüber informiert, dass ich diese Einwilligung jederzeit ohne Nachteile widerrufen kann. Mir ist bewusst, dass aus Gründen der Nachvollziehbarkeit der Vorgang der Einwilligung selbst mitprotokolliert wird. Von der <Bezeichnung des Verantwortlichen> wurde mir versichert, dass meine datenschutzrechtlichen Belange ohne Einschränkung gewährleistet werden.

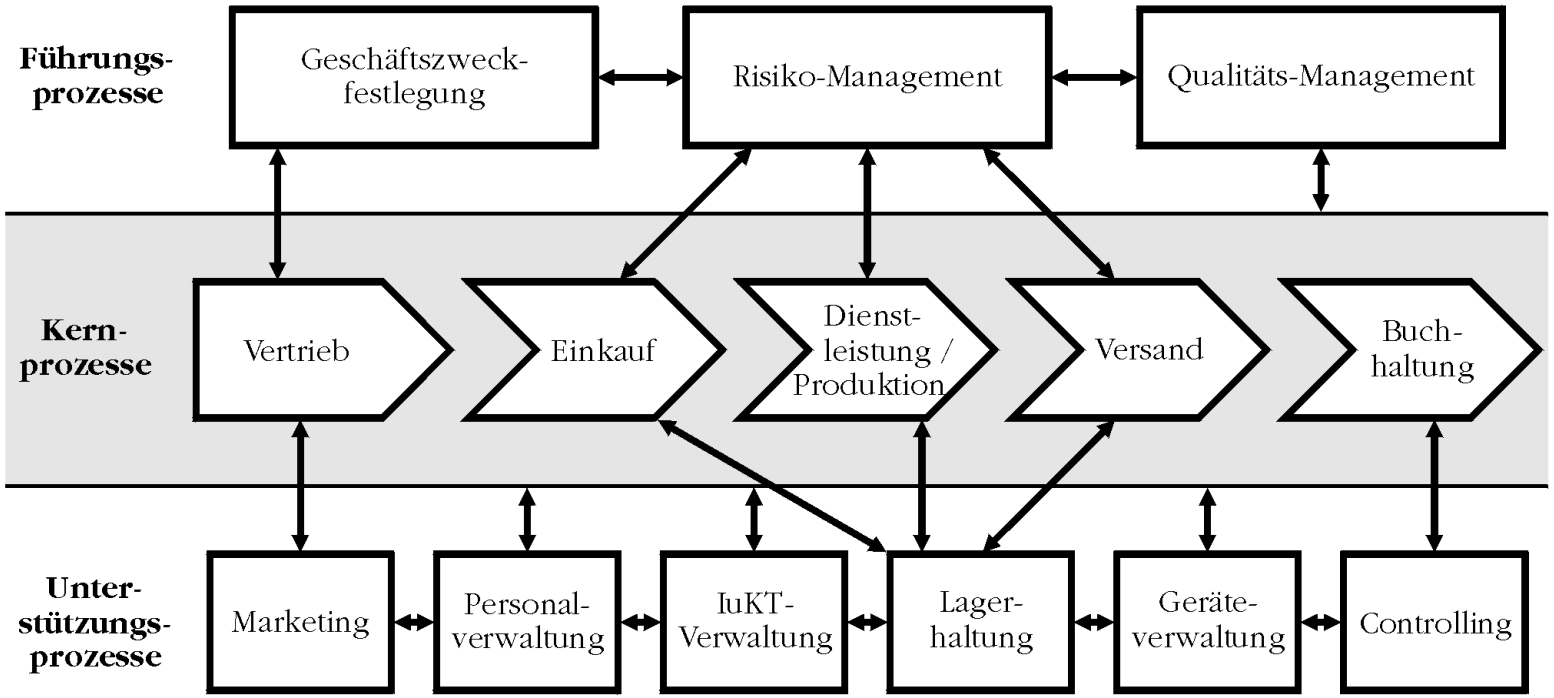
☐ Obiger Einwilligungserklärung stimme ich zu! *(bitte Häkchen setzen)*

☒ *Absenden!*

3.5 Verfahren I

Aufgabe:

- Für ein Unternehmen wurde folgende Prozesslandkarte ermittelt:



3.5 Verfahren II

Aufgabe:

- Zählen Sie je fünf grundlegende **Verfahren zur Verarbeitung personenbezogener Daten** auf, die von diesem Unternehmen damit im Einsatz sind zur
  a) Verarbeitung personenbezogener Beschäftigtendaten
  b) Verarbeitung personenbezogener Kundendaten

3.5 Verfahren

Beschäftigtendaten-verarbeitung

Personalverwaltung:

- Bewerbungsverfahren
- Personalaktenführung
- Arbeitszeitüberwachung

Buchhaltung:

- Lohn- und Gehaltsabrechnung

Dienstleistung / Produktion:

- Betriebsdatenerfassung

Qualitäts-Management:

- Qualitätskontrolle

Controlling:

- Leistungskontrolle

IuKT-Verwaltung:

- Elektronische Kommunikation

Kundendaten-verarbeitung

Marketing:

- Kundengewinnung (Messen & Gewinnspiele)
- Kundenbewerbung & Newsletter
- Kundendatenanalyse (Tracking)

Vertrieb:

- Vertragsabwicklung
- Customer Relationship Management

Buchhaltung:

- Zahlungsüberwachung

Versand:

- Versand

IuKT-Verwaltung:

- Elektronische Kommunikation