Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 3. Übung im SoSe 2017:
Mitarbeiterdatenschutz (1)

3.1 Mitbestimmung

Aufgabe:

- Ein Unternehmen, das über einen Betriebsrat verfügt, möchte eine Arbeitszeitüberwachung einführen (Arbeitszeiten, Krankheitsausfallzeiten, Weiterbildungszeiten, unproduktive Zeiten). Welche Anforderungen aus der EU-DSGVO, § 32 BDSG und BetrVG hat das Unternehmen dabei zu beachten?

3.1 Mitbestimmung (1)

- **Arbeitszeitüberwachung = Verhaltenskontrolle**
  → Verhaltenskontrolle = Profiling nach Art. 4 Nr. 4 EU-DSGVO
  → Datenschutz-Folgenabschätzung nötig nach Art. 35 Abs. 3 lit. a EU-DSGVO
  → Mitbestimmung nach § 87 Abs. 1 Nr. 1 BetrVG, da Arbeits-zeit-Verhalten der Arbeitnehmer im Betrieb Gegenstand ist, und ggf. nach § 87 Abs. 1 Nr. 6 BetrVG, wenn das Arbeits-zeit-Verhalten mittels technischer Einrichtung überwacht wird, die zur Überwachung auch bestimmt ist (hierzu keine nähere Angabe in der Aufgabe)
  → Nach § 80 Abs. 2 BetrVG ist der Betriebsrat vom Arbeitgeber rechtzeitig & umfassend über geplante Einführung zu unter-richten (bzw. nach § 90 Nr. 2 BetrVG im Fall der technischen Einrichtung)

3.1 Mitbestimmung (2)

- Arbeitszeitüberwachung = Verfahren zur Durchführung des Beschäftigungsverhältnisses (Einhaltung arbeitsvertraglich vereinbarter Arbeitszeiten)
  → Rechtsgrundlage: § 32 Abs. 1 BDSG
  → Beteiligungsrechte des Betriebsrats bleiben nach § 32 Abs. 3 BDSG unberührt
  → trotz gesetzlicher Regelung besteht Mitbestimmung nach § 87 Abs. 1 BetrVG fort
  → Betriebsrat kann insbesondere den Datenschutzbeauftragten als Sachverständigen nach § 80 Abs. 3 BetrVG hinzuziehen
- Üblicherweise wird zu diesem Verfahren eine Betriebsvereinbarung zwischen Betriebsrat und Arbeitgeber vereinbart

3.1 Mitbestimmung (3)

- Weitere Anforderungen:
  - ° Nur erforderliche Arbeitszeitdaten erheben und verwenden
  - ° Arbeitszeitdaten unterliegen grundsätzlich der Zweckbindung, Zweckänderungen würden einer Abwägung nach Art. 6 Abs. 1 lit. f EU-DSGVO bedürfen
  - ° Ergreifung ausreichender technischer & organisatorischer Maßnahmen nach Art. 32 EU-DSGVO
  - ° Aufbewahrung der Arbeitszeiten gemäß gesetzlicher Fristen (6 Jahre nach § 147 Abs. 1 Nr. 5 AO)

3.1 Mitbestimmung (4)

- Weitere Anforderungen (Ergänzung außerhalb der Übung):
  ° Aufgrund der spezifischen Aufbewahrungsfrist aus § 16 Abs. 2 ArbZG sind Überstunden ab 2 Jahren weiterhin zu speichern nach Art. 17 Abs. 3 lit. b EU-DSGVO (wg. der AO-Vorgabe)
  ° Aufgrund der spezifischen Aufbewahrungsfrist aus § 3 Abs. 1 Nr. 2 EntgFG sind Daten über Arbeitsunfähigkeiten nach 1 Jahr weiterhin zu speichern nach Art. 17 Abs. 3 lit. b EU-DSGVO (wg. der AO-Vorgabe)
  ° Daten über Arbeitsunfähigkeiten = Gesundheitsdaten (Daten über zeitweise nicht vorhandener Gesundheit)
  → nötig zur Rechtsausübung des Arbeitgebers im Sinne von Art. 9 Abs. 2 lit. b EU-DSGVO (Ausgleichszahlungen durch Krankenkassen)

3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (I)

Aufgabe:

- Das Unternehmen aus 3.1 möchte am Betriebsrat vorbei ein System zur Personalentwicklung einführen. Die Personalabteilung möchte damit folgende Wünsche umsetzen:
  ° Anhand der im Bewerbungsverfahren eingereichten Zeugnisse soll ermittelt werden, welcher Fortbildungsbedarf anhand der zugeordneten Stellenbeschreibung für erfolgreiche Bewerber besteht.
  ° Die Arbeitszeitdaten aus der Arbeitszeitüberwachung sollen mit den Produktivitätsdaten, die bereits im Rahmen der Betriebsdatenerfassung erhoben wurden, im Sinne von Leistungsdaten korreliert werden, um feststellen zu können, welche Mitarbeiter besonders produktiv sind.
  ° Ermittelte Leistungsdaten sollen in den einzelnen Produktionsbereichen als Top 10 ausgehängt werden, um so Nichtplatzierte zu höheren Leistungen zu motivieren.
  ° Anhand der Daten aus den jährlichen Mitarbeitergesprächen soll ermittelt werden, welche Mitarbeiter für spezialisierte Aufgaben, insbesondere zur Teamleitung, geeignet sind und welche Fortbildungsmaßnahmen dafür notwendig sind.

3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (II)

Aufgabe:

- ° Zu jeder Fortbildung haben die Mitarbeiter Bewertungen anzugeben, wie nützlich und wie teuer genossene Fortbildungen waren.
  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.

3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (1)

A) Ermittlung potenzieller Datenschutzrisiken:

- Personalentwicklung am Betriebsrat vorbei
  1. Verletzung Mitbestimmungsrecht → strafbare Behinderung der Tätigkeit des Betriebsrats (§ 119 Abs. 1 Nr. 2 BetrVG)
     → weder notwendig, noch verhältnismäßig nach Art. 35 Abs. 7 lit. b EU-DSGVO
  2. Infolge der Nichtbeachtung des Mitbestimmungsrechts unzulässiges Verfahren
     → Verfahren nicht begründbar nach Art. 6 Abs. 1 lit. f EU-DSGVO
     → weder notwendig, noch verhältnismäßig nach Art. 35 Abs. 7 lit. b EU-DSGVO
     → Bußgeld nach Art. 83 Abs. 5 lit. a EU-DSGVO möglich
- Auswertung Zeugnisdaten (Fähigkeitsdaten) für Fortbildungsbedarf
  3. Zweckänderung von Fähigkeitsdaten ohne Abwägung
     → neuer Zweck aber mit altem vereinbar im Sinne von Art. 6 Abs. 4 EU-DSGVO
     → notwendig, um Personal optimal einsetzen zu können, und auch verhältnismäßig nach Art. 35 Abs. 7 lit. b EU-DSGVO
     → formaler Verstoß, da noch keine Verletzung (wg. Planung)

3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (2)

A) Ermittlung potenzieller Datenschutzrisiken:

- Abgleich mit Leistungsdaten aus Betriebsdatenerfassung
  4. Zweckänderung von Leistungsdaten ohne Abwägung
     → neuer Zweck aber mit altem vereinbar im Sinne von Art. 6 Abs. 4 EU-DSGVO
     → Notwendigkeit fraglich, wenn z.B. nicht durch Betriebsvereinbarung abgesichert (Leistungsprämien), und damit auch nicht verhältnismäßig nach Art. 35 Abs. 7 lit. b EU-DSGVO
     → formaler Verstoß, da noch keine Verletzung (wg. Planung)
- Aushang der Leistungsdaten (= Veröffentlichung einer sog. „Rennliste“)
  5. Unbefugte Übermittlung von Leistungsdaten
     → Leistungsdaten = Profiling nach Art. 4 Nr. 4 EU-DSGVO (Arbeitsleistung)
     → Verstoß gegen Art. 22 Abs. 1 EU-DSGVO
     → Bußgeld nach Art. 83 Abs. 5 lit. b EU-DSGVO
- Auswertung Mitarbeitergespräche für Personalentwicklung → ordnungsgemäß!
- Bewertung erhaltener Fortbildungen → ggf. potenzieller Neidfaktor (außerhalb DS!)

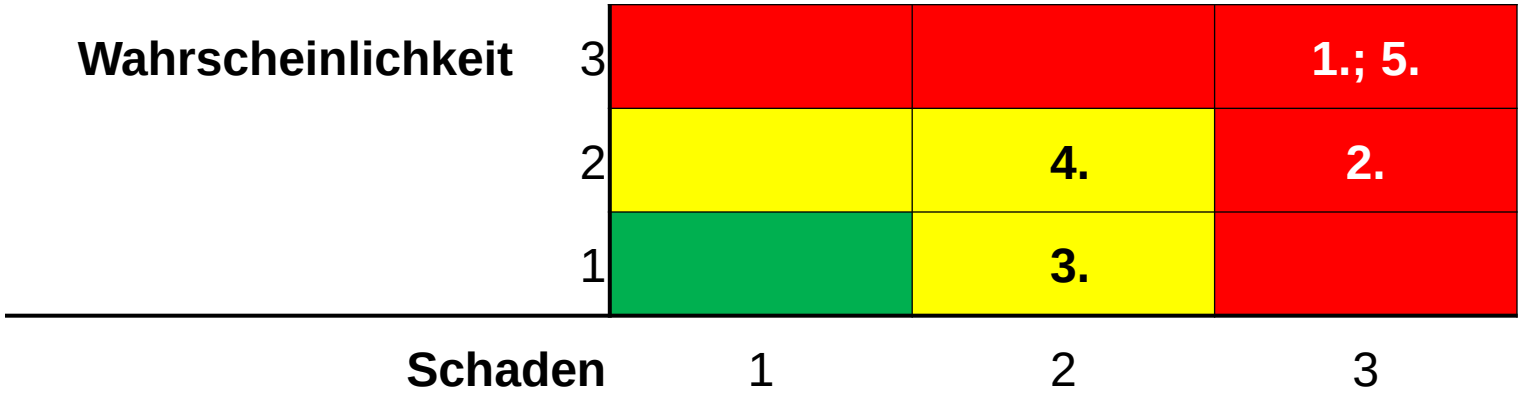
3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (3)

B) Abschätzung der Eintrittsstufe:

1. Verletzung Mitbestimmungsrecht: Eintritt sicher, da auch Betriebsratsmitglieder von Verfahren betroffen sind
2. Infolge der Nichtbeachtung des Mitbestimmungsrechts unzulässiges Verfahren: Eintritt wahrscheinlich, da zugleich mit Mitbestimmungsverstoß verbunden
3. Zweckänderung von Fähigkeitsdaten ohne Abwägung: Eintritt möglich, aber unwahrscheinlich (zulässige Datenverwendung, wenn mit Abwägung durchgeführt)
4. Zweckänderung von Leistungsdaten ohne Abwägung: Eintritt wahrscheinlich, da Leistungskontrolle der Mitbestimmung unterliegt
5. Unbefugte Übermittlung von Leistungsdaten: Eintritt sicher, da innerbetriebliche Veröffentlichung von allen Betroffenen ausdrücklich zur Kenntnis genommen werden soll

→ Bewertung der Risiken nach Art. 35 Abs. 7 lit. c EU-DSGVO nach Risk-Map:

3.2 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)

3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (5)

C) Handlungsempfehlung für Abhilfemaßnahmen (nach Art. 35 Abs. 7 lit. d EU-DSGVO)**:**

1. Verletzung Mitbestimmungsrecht
   → Betriebsrat einbeziehen!
2. Infolge der Nichtbeachtung des Mitbestimmungsrechts unzulässiges Verfahren
   → durch Maßnahme zu 1. erledigt
3. Zweckänderung von Fähigkeitsdaten ohne Abwägung
   → Abwägung vornehmen
4. Zweckänderung von Leistungsdaten ohne Abwägung
   → Abwägung vornehmen & Betriebsrat einbeziehen
5. Unbefugte Übermittlung von Leistungsdaten
   → unterlassen, da unverhältnismäßiger Eingriff!

3.2 Datenschutzrisiko gemäß Datenschutz-Folgenabschätzung (6)

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 hier verzichtet, da dies nicht eindeutig aus der Aufgabenstellung hervor geht

3.3 Digitalisierung von Personalakten

Aufgabe:

- Ein Unternehmen möchte seine bisher auf Papier geführten Personalakten digitalisieren. Welche technischen und organisatorischen Maßnahmen sollte das Unternehmen im Sinne von Art. 32 EU-DSGVO dabei ergreifen, damit die digitalen Personalakten einem angemessenen Schutz unterliegen? Berücksichtigen Sie dabei, dass sich in den Personalakten besondere Arten personenbezogener Daten, Kontodaten und Persönlichkeitsprofildaten befinden.

3.3 Digitalisierung von Personalakten (1)

- Personalakten beinhalten üblicherweise folgende Datenkategorien: Namensdaten, Bilddaten, sonstige Identifikationsdaten, Kontaktdaten, Bewerbungsdaten, Qualifikationsdaten (über berufliche Fortbildung, erhaltene Einweisungen, etc.), Vertragsdaten (zum Anstellungsvertrag, inkl. Personalverwaltungsdaten wie Personalnummer, Stellenbezeichnung, Zuordnung zur Organisationseinheit, Steuerdaten, Krankenversicherungsdaten, Daten über Bankkonto, Schwerbehinderungsgrad etc.), Leistungsdaten (sofern Leistungsprämien oder dgl.), Verhaltensdaten (für den Fall von Abmahnungen)
  → **hoher Schutzbedarf** der zu speichernden Daten, so dass Verarbeitung eher ein höheres Risiko für die Rechte und Freiheiten der Beschäftigten zur Folge haben kann

3.3 Digitalisierung von Personalakten (2)

Maßnahmen zur innerbetrieblichen Organisation:

- Bestellung eines Datenschutzbeauftragten
- Schulung der Zugriffsbefugten über Datenschutz

Maßnahmen zur Vertraulichkeit:

- Verpflichtung der Zugriffsbefugten auf Vertraulichkeit
- Personalbereich & Serverraum getrennte Sicherheitszonen
- Personalbüros in Abwesenheit der HR-Mitarbeiter verschlossen
- Vergabe nur erforderlicher Zutrittsbefugnisse
- Temporäre Zugriffsgewährung (für Betroffenen vollständig und für Vorgesetzte nur anteilig) unter Anwesenheit von HR-Mitarbeitern
- Protokollierung erfolgter Einsichtnahmen in die Personalakte

3.3 Digitalisierung von Personalakten (3)

Maßnahmen zur Vertraulichkeit & Verfügbarkeit:

- Serverraum nur mit Chipkarte betretbar unter Aufzeichnung des Zutritts
- Vergabe von Zugangsbefugnissen nur für Befugte
- Authentifikation mittels personalisierter Benutzerkennung und ausreichend langem & komplexen Passwort
- Einsatz einer Bildschirmsperre bei 15 minütiger Inaktivität
- Regelmäßige Prüfung der eingeräumten Zugangsbefugnisse
- Unverzüglicher Zugangsrechteentzug bei vorliegender Nicht-erforderlichkeit
- Fehldrucke digitaler Personalakten sind unter Einhaltung der DIN 66399 Stufe P-4 zu vernichten

3.3 Digitalisierung von Personalakten (4)

Maßnahmen zur Vertraulichkeit & Integrität:

- Einsatz eines detaillierten Berechtigungskonzepts mit klarer Beschränkung vergebener Zugriffsrechte
- Unterscheidung von Zugriffsbefugnissen nach Unterlagenarten, z.B. besonderer Zugriffsschutz auf Schwerbehindertenunterlagen
- Regelmäßige Prüfung der eingeräumten Zugriffsrechte
- Unverzüglicher Zugriffsrechteentzug bei vorliegender Nichterforderlichkeit
- Zugriffsrechte für Betroffene und Vorgesetzte umfassen keine Exportrechte, sondern nur Anzeigerechte (und Druckrechte)

3.3 Digitalisierung von Personalakten (5)

Maßnahmen zur Verfügbarkeit & Belastbarkeit:

- Papierne Personalunterlagen, die nach § 2 Abs. 1 NachwG (und anderen spezialrechtlichen Auflagen) schriftlich vorzuhalten sind, werden ergänzend auf Papier vorgehalten
- Datenbank mit Personalaktendaten redundant auslegen
- Personalaktendaten sind täglich auf Backups zu sichern
- Backupdaten werden in einem anderen Brandabschnitt gelagert
- Regelmäßige Prüfung der Wirksamkeit der Datensicherung
- Server mit ausreichend dimensionierter USV betrieben

3.3 Digitalisierung von Personalakten (6)

Maßnahmen zur Belastbarkeit:

- Server mit Firewall und Netzwerksegregation gesichert
- Export für andere Anwendungen (z.B. Lohn- und Gehaltsdaten-übeweisung) nur über dedizierte Schnittstellen
- Remote-Zugriff auf digitalisierte Personalakten nur nach Freigabe durch zuständigen HR-Mitarbeiter mit Interventionsrecht des HR-Mitarbeiters (darf Verbindung trennen)
- Personalaktendaten werden in unterschiedliche Segmente aufgeteilt (Stammdaten, Bewerbungsdaten, Exportdaten, Gesundheitsdaten, …)

3.4 Videoüberwachung

Aufgabe:

- Ein Unternehmen möchte aufgrund festgestellter Unregelmäßigkeiten eine Videoüberwachung einführen. Wie beurteilen Sie die beiden Varianten aus datenschutzrechtlicher Sicht?
  A) Der Arbeitgeber ist der Überzeugung, dass Mitarbeiter Arbeitszeitbetrug durchführen und einen nennenswerten Anteil der vorgesehenen Arbeitszeit für Rauchpausen verwenden. Daher soll der Eingangsbereich des Gebäudes aufgezeichnet werden.
  B) Der Arbeitgeber hat festgestellt, dass produzierte Güter, die vom Unternehmen vertrieben werden, einen unerklärlichen Schwund aufweichen. Um feststellen zu können, welche Mitarbeiter für diesen Schwund verantwortlich sind, sollen folgende Arbeitsbereiche aufgezeichnet werden: Produktionsstrecke, Lager, Versand, Umzugsräume.
  Gehen Sie bei Ihrer Lösung davon aus, dass die Videoüberwachung offen erfolgen soll (also nicht heimlich). Begründen Sie Ihre Antwort!

3.4 Videoüberwachung (1)

Videoüberwachung = Verhaltensaufzeichnung = Profiling

Fall A) Videoüberwachung an Eingangstüren zur Aufdeckung von Arbeitszeitbetrug

- Aufzeichnung von Videodaten an Eingangstüren = öffentlich zugänglicher Raum
- Arbeitszeitbetrug stellt sogar eine Straftat nach § 263 Abs. 1 StGB dar!
- Arbeitszeitbetrug = Straftat im Beschäftigungsverhältnis nach § 32 Abs. 1 BDSG
- Aufdeckung von Arbeitszeitbetrug = Wahrnehmung berechtigter Interessen nach Art. 6 Abs. 1 lit. f EU-DSGVO
- Konkreter Zweck = Beweissicherung zu vermutetem Arbeitszeitbetrug (ggf. führt festgestellter Arbeitszeitbetrug zur Anzeige und/der außerordentlichen Kündigung des überführten Beschäftigten!)
- (Überbordende) Rauchpausen während der Arbeitszeit führen dazu, dass in dieser Zeit keine Arbeitsleistung erbracht wird → Verhältnismäßigkeit beachten
- In der Aufgabe gab‘s aber keine Angabe, ob sich Beschäftigte zur Rauchpause „ausstempeln“ → Annahme: es erfolgt kein „Ausstempeln“ zur Rauchpause

3.4 Videoüberwachung (2)

Fall A) Videoüberwachung an Eingangstüren zur Aufdeckung von Arbeitszeitbetrug

- Nach Art. 6 Abs. 1 lit. f EU-DSGVO ist die Videoüberwachung nur zulässig, wenn die Aufzeichnung der Videodaten erforderlich ist (Aufzeichnung des Rauchens als Beweis insoweit tauglich – ggf. i.V.m. Stempeldaten) und diesem keine überwiegenden Interessen der Betroffenen entgegenstehen → Abwägung nötig!
- Bei der Abwägung zählt als Betroffeneninteresse:
  ° Videoüberwachung = Profiling → Datenschutz-Folgenabschätzung nötig
  ° Raucherdaten = indirekte (!) Gesundheitsdaten nach Art. 4 Nr. 15 EU-DSGVO
  ° Betroffene haben Interesse an unbeobachteter Pause
  ° Pausenzeiten als Ruhepausen nach § 4 ArbZG gefordert (Pause dient zur Regeneration) → Rauchen während dieser Ruhepause kein Arbeitszeitbetrug
  ° Für Nachweis von Arbeitszeitbetrug ggf. längerfristige Aufzeichnung nötig
- Kein überwiegendes Betroffeneninteresse nur gegeben, wenn obigen Einschränkungen (in Rahmen der Datenschutz-Folgenabschätzung) gebührend Rechnung getragen wird! Ansonsten wäre Videoüberwachung unzulässig, da unverhältnismäßig!

3.4 Videoüberwachung (3)

Fall B) Videoüberwachung ausgewählter Räume zur Aufdeckung von Diebstahl

- Produktionsstrecke, Lager & Versand = öffentlich nicht-zugänglicher Raum
  → Art. 6 Abs. 1 lit. f EU-DSGVO als Rechtsgrundlage mit entsprechender Abwägung, allerdings verschärft, da öffentlich nicht-zugänglicher Raum
- Umzugsräume = Sozialraum, Aufzeichnung nach SG-Urteil v. 1990 unzulässig!
  → für weitere Aufgabe auf Produktionsstrecke, Lager & Versand beschränkt
- Diebstahl = Straftat nach § 242 Abs. 1 BDSG
- Diebstahl produzierter Güter = Straftat im Beschäftigungsverhältnis nach § 32 Abs. 1 BDSG
- Aufdeckung des innerbetrieblichen Diebstahls berechtigtes Interesse
- Bei der Abwägung nach Art. 6 Abs. 1 lit. f EU-DSGVO zählt als Betroffeneninteresse:
  ° Videoüberwachung = Profiling → Datenschutz-Folgenabschätzung nötig
  ° Aufzeichnung der gesamten Arbeitstätigkeit = starker Eingriff in das informationelle Selbstbestimmungsrecht (Beschäftigter kann sich Eingriff nicht entziehen!) → Vollkontrolle unzulässig (BAG-Beschluss v. 2004)
  → nur kurze Aufzeichnungsdauer; besser: Güter mit RFID-Chip versehen

3.5 Gestaltung ERP-System

Aufgabe:

- Im eingesetzten ERP-System eines Unternehmens werden folgende Verfahren abgewickelt:
  ° Betriebsdatenerfassung zur Erhebung der Produktionsdaten (in welcher Produktionsstätte wurde welcher Teil des gefertigten Produkts mit welchem Zeitaufwand von welchem Mitarbeiter gefertigt?)
  ° Lagerstättenverwaltung zur Lagerung der Roh-, Hilfs- und Betriebsstoffe, der unfertigen Erzeugnisse, der gefertigten Produkte und der Kommissionierung für den Versand mittels RFID-Chips
  ° Finanzbuchhaltung zur Dokumentation aller finanzwirksamen Vorgänge
  ° Vertrieb von Produkten, wobei Mitarbeiter einen Mitarbeiterrabatt erhalten
  Für die Betriebsdatenerfassung, die Finanzbuchhaltung und den Vertrieb importiert das ERP-System Daten aus dem eingesetzten HR-System. Worauf muss aus Ihrer Sicht das Unternehmen bei der Gestaltung des ERP-Systems aus datenschutzrechtlichen Gründen achten? Begründen Sie Ihre Antwort!

3.5 Gestaltung ERP-System (1)

- ERP-System = System, mit dem eine Vielzahl verschiedener Verfahren durchgeführt wird:
  - ° Betriebsdatenerfassung = Verfahren zur Leistungskontrolle (→ Profiling!)
  - ° Lagerstättenverwaltung = Verfahren zur potenziellen (Kommissionierungs-) Verhaltenskontrolle (Bewegungsprofil → Profiling!)
  - ° Finanzbuchhaltung = Verfahren zur Abwicklung rechtsgeschäftlicher Schuldverhältnisse (hier: wegen Mitarbeiterrabatten nicht nur hinsichtlich der Lohn- & Gehaltsdaten, sondern auch hinsichtlich der Verkäufen unter Berücksichtigung von Mitarbeiterrabatten)
  - ° Vertrieb = Verfahren zur Abwicklung rechtsgeschäftlicher Schuldverhältnisse (hier: bei Mitarbeiterrabatten mit Bezug zu Mitarbeitern)
  - → (zweckbezogene) Datentrennung erforderlich (logische Datentrennung)!
- Bis auf die Lagerstättenverwaltung werden (Stamm-) Daten aus HR-System importiert
  - → Schnittstellen absichern!
  - → Importdaten auf notwendiges Minimum reduzieren! (wg. Art. 5 Abs. 1 lit. c EU-DSGVO)

3.5 Gestaltung ERP-System (2)

- Aufgrund der Fülle der Verfahren, die mittels des ERP-Systems abgewickelt werden und jeweils der Datenschutz-Folgenabschätzung bedürfen, und dem Umfang der darin gespeicherten Daten hat ERP-System einen **hohen Schutzbedarf**
  → umfassende Schutzmaßnahmen nach Art. 32 EU-DSGVO erforderlich!
  → für Profiling Betriebsvereinbarung abschließen (Art. 22 Abs. 2 lit. b EU-DSGVO), dann Verarbeitung nach Art. 6 Abs. 1 lit. c EU-DSGVO möglich ohne Einholung einer Einwilligungserklärung (die BV muss aber wiederum den Anforderungen der EU-DSGVO genügen)
  → Verarbeitung muss nach Treu und Glauben erfolgen (Art. 5 Abs. 1 lit. a EU-DSGVO (auch bei BV-Basis nach Art. 6 Abs. 2 EU-DSGVO)
  → bei RFID-Chips Pseudonymisierung nach Art. 4 Nr. 4 EU-DSGVO beachten!