Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2015:
Mitarbeiterdatenschutz (3)

4.1 Bring your own Device

Aufgabe:

- Ein Unternehmen möchte seinen Mitarbeitern gestatten, eigene Smart Phones für dienstliche Aufgaben zu verwenden (Stichwort: Bring Your Own Device). Welche datenschutzrechtlichen und datensicherheitstechnischen Gesichtspunkte sind bei der Entscheidung, ob BYOD eingeführt werden soll, aus Ihrer Sicht maßgeblich?

4.1 Bring your own Device (1)

- Durch eine Gestattung der Verwendung privater Smart Phones zu dienstlichen Zwecken wäre es zulässig, betriebliche Vorgänge über private Endgeräte abzuwickeln
- Unter diesen Umständen ist die Verabschiedung einer verbindlichen Richtlinie erforderlich, die im Einzelnen regelt, welche betrieblichen Vorgänge mittels des privaten Smart Phones auf welche Weise ausgeführt werden dürfen, da andernfalls keinerlei betriebliche Kontrolle über betriebliche Vorgänge besteht
- Auf privatem Smart Phone werden mit hoher Wahrscheinlichkeit dienstliche Kontaktdaten abgelegt
  → soweit nicht virtuell getrennt gespeichert, „wechselt“ verantwortliche Stelle
  → Kontaktdaten werden im datenschutzrechtlichen Sinne übermittelt!
  → Abwägung erforderlich! (kann zweckmäßigerweise nur vorab erfolgen und führt im Ergebnis zu Auflagen, die in Richtlinie aufzunehmen sind)
  → Vorabkontrolle erforderlich, zumal besonderes Risiko gegeben, wenn z.B. auf privaten Smart Phones Apps eingesetzt werden, die Kontaktdaten weiterleiten, oder gar Jailbreak durchgeführt wurde

4.1 Bring your own Device (2)

- Sollen neben den betrieblichen Kontaktdaten noch weitere betrieblichen Daten über das private Smart Phone abrufbar sein (z.B. Mails), sind weitergehende Schutzvorkehrungen erforderlich (i.d.R. nur sinnvoll darstellbar, wenn eine virtuell getrennte Oberfläche mit Virenschutz oder zumindest eine SSL-verschlüsselter Zugang eingerichtet wurde; zudem unkontrollierten Informationsabfluss verhindern)
- Mitarbeiter, der privates Smart Phone nutzen darf, muss Zusicherungen abgeben, insbesondere zum PIN-Schutz und zur Nichtweitergabe des Smart Phones an Dritte
- Bei Anschluss des Smart Phones an das LAN sind die Regeln anzuwenden, die für den Anschluss betriebsfremder Endgeräte gelten (kein unkontrollierter Datentransfer von oder zum Endgerät, Download von Daten aus Smart Phone nur nach beanstandungsfreier Malwareprüfung)

4.2 Nutzung Smart Phones

Aufgabe:

- Ein Unternehmen möchte hinsichtlich dienstlich ausgegebener Smart Phones Nutzungsvorgaben zu deren Verwendung verabschieden. Was sollte das Unternehmen aus datenschutzrechtlichen und datensicherheitstechnischen Gründen wie regeln?

4.2 Nutzung Smart Phones

- **Umfang zulässiger Privatnutzung**, ggf. unterschiedlich für
  ° Telefonieren
  ° Surfen
  ° Abrufen dienstlicher Mails
  ° Fotographieren
  → Geltung des Grundrechts auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme
- **Berechtigung zur Installation von Apps**
  → Whitelist- oder Blacklist-Verfahren
  → bei wirksamer Auftrennung in dienstliches & privates Segment, sofern Privatnutzung gestattet wurde
- **Berechtigung zum Anschluss externer Datenträger**
- **Umfang der betrieblichen Kontrolle**
  → Einzelverbindungsnachweise zur Kostenkontrolle
  → Protokollierung von Aktivitäten
- **Hinterlegung der PUK** (und ggf. auch der PIN)
- **Verbot des Umgehens voreingestellter Sicherheitsfunktionen**

4.3 Privacy Impact Assessment I

Aufgabe:

- Ein Unternehmen möchte die monatliche Mitteilung über die erfolgte Gehaltszahlung an seine Beschäftigten nicht mehr auf Papier ausgeben, sondern mittels App abrufen lassen. Zu diesem Zweck soll eine entsprechende App programmiert werden, die alle datenschutzrechtlichen Anforderungen erfüllen soll. Führen Sie ein Privacy Impact Assessment (PIA) durch, um Vorgaben für die Durchführung der Programmierarbeiten zu ermitteln.

4.3 Privacy Impact Assessment II

- Hinweis: Ausgehend von den Datenarten, die im Verfahren zur Lohn- und Gehaltsabrechnung anfallen (siehe auch Aufgabe 2.1), und möglichen Zugriffsbefugnissen ist im Rahmen der PIA darzustellen, welche Auswirkung welcher App-Aspekt auf den Betroffenen hinsichtlich datenschutzrechtlicher Anforderungen aus dem BDSG, der besonderen Vertrauensstellung gegenüber der verantwortlichen Stelle und der Reputation vor allem für den Fall einer Datenpanne haben kann und welche Maßnahmen nötig sind, um den Eintritt einer ungewollten Auswirkung vermeiden zu können. Bei den zu verfolgenden Zielen ist es hilfreich, die rechtlichen Anforderungen als Leitsätze zu formulieren (siehe auch Aufgabe 1.4). Die verschiedenen App-Aspekte sollten sich an Programmierschritten, Schnittstellen (siehe auch Aufgabe 3.3) und Kernfunktionen (Datenvalidierung, Zugriffsmanagement, Datenverfügbarkeit, Störfallmanagement, Protokollierung, Netzwerksicherheit, Trennung der Entwicklungsumgebung von der Testumgebung und Einsatzumgebung sowie Schwachstellenmanagement) orientieren.

4.3 Privacy Impact Assessment (1)

- Nach Aufgabe 2.1 werden im Verfahren zur Lohn- und Gehaltsabrechnung folgende **Datenkategorien** automatisiert verarbeitet:
  Namensdaten, sonstige Identifikationsdaten, Vertragsdaten (zum Anstellungsvertrag, inkl. Personalverwaltungsdaten wie Personalnummer, Stellenbezeichnung, Zuordnung zur Organisationseinheit, Steuerdaten, Krankenversicherungsdaten, Daten über Bankkonto, Schwerbehinderungsgrad, etc.), Leistungsdaten (sofern Leistungsprämien oder dgl.)
- Von diesen Datenkategorien sind **für den Betroffenen** aufgrund **potenzieller Folgen** von besonderer Bedeutung:
  - Identifikationsdaten (Name, Geburtsdatum, Adressdaten) → Verwendbar für **Identitätsdiebstahl & Social Engineering** (→ evtl. Vermögensschaden)
  - Steuerdaten (Steuer-ID, Bruttogehalt, Steuerklasse, Konfession) → Angabe über potenziell vorhandenes Vermögen (→ Attraktivität als Angriffsziel)
  - Krankenversicherungsdaten (Sozialversicherungsnummer, Krankenkasse) → teilweise interpretierbar als Angabe über sozialen Status (dto)
  - Daten über Bankkonto (Bank, Kontonummer) → Eignung für unbefugte Lastschriftbelastung → **potenzieller Vermögensschaden**

4.3 Privacy Impact Assessment (2)

- Laut Aufgabenstellung ist geplant, dass die monatliche Gehaltsübersicht künftig mittels einer App abrufbar sein soll, wobei dieser Abruf die monatliche Verteilung der Gehaltsübersichten ersetzen soll.
- Exkurs: Nach § 108 Abs. 1 GewO ist dem Arbeitnehmer bei Zahlung des Arbeitsentgelts eine Abrechnung in Textform zu erteilen, wobei in der Entgeltbescheinigungsverordnung im Einzelnen aufgelistet ist, welche Angaben dabei anzugeben sind. Der Abruf vermittels der App ist insoweit also auch dazu geeignet, dem Beschäftigten die Entgeltabrechnung in Textform nach § 126b BGB bereitzustellen. Hierzu muss die an ihn gerichtete Erklärung so gespeichert werden, dass sie ihm während eines für ihren Zweck angemessenen Zeitraums zugänglich ist und unveränderlich wiedergegeben wird.
- Hinsichtlich **potenzieller Zugriffe** sind daher im Rahmen der Entwicklung und der anschließenden Inbetriebnahme der App zu beachten:
  - Entwicklung der App → **Entwicklungsumgebung**
  - Test der Funktionstüchtigkeit und Sicherheit der App → **Testumgebung**
  - Schnittstellen zum Gehaltsbuchhaltungssystem → **Einsatzumgebung**
  - App und lokaler Speicher bei Smartphone & Tablet → **Einsatzumgebung**

4.3 Privacy Impact Assessment (3)

- Ausgehend von den in Aufgabe 1.4 ermittelten Leitsätzen zum Datenschutz sind bei Entwicklung, Testen und Einsatz der App folgende **Ziele** relevant:
  - Datenverarbeitungssysteme sind so auszuwählen bzw. zu gestalten, dass möglichst wenig personenbezogene Daten von diesem System automatisiert verarbeitet werden (**Datensparsamkeit**)
  - Beschäftigte, die mit personenbezogene Daten umgehen, sind während dieser Tätigkeit und auch nach deren Beendigung darauf verpflichtet, diese Daten nur befugt zu erheben, verarbeiten oder nutzen (**Datengeheimnis**)
  - Nur Befugte dürfen Datenverarbeitungssysteme nutzen (**Zugangsschutz**)
  - Zugriffe auf personenbezogene Daten sind auf Berechtigte beschränkt (**Zugriffsschutz**)
  - Bei der Weitergabe personenbezogener Daten muss stets nachprüfbar sein, an wen die Daten weitergegeben wurden (**Weitergabeschutz**)
  - Personenbezogene Daten sind vor zufälliger Zerstörung oder Verlust zu schützen (**Verfügbarkeitsschutz**)

4.3 Privacy Impact Assessment (4)

- Eine App ist ein Telemediendienst → TMG einschlägig; da dieser Dienst zur Gehaltsmitteilung jedoch offensichtlich zu ausschließlich beruflichen Zwecken im Arbeitsverhältnis eingesetzt wird, ist nach § 11 Abs. 1 Nr. 1 TMG der Abschnitt zum Datenschutz nicht gültig. Die datenschutzrechtlichen Anforderungen ergeben sich damit aus dem subsidiären BDSG.
- Als Programmierschritte dienen üblicherweise nach dem Wasserfallmodell:
  - Spezifikation der Anforderungen für die App (Lastenheft → WAS)
  - Design der App (Pflichtenheft → WIE)
  - Feinkonzept und Programmierung (Implementation)
  - Funktionstest
  - Einsatz der App
- Laut Aufgabe 3.3 bestehen für die Gehaltsabrechnung folgende Schnittstellen:
  - Finanzbuchhaltung im ERP-System
  - Stammdatenimport aus HR-System
- Die App dagegen liest jedoch nur die Daten aus der Gehaltsabrechnung aus und führt nicht die Gehaltsabrechnung durch → Vermeidung verdeckter Kanäle!

4.3 Privacy Impact Assessment (5)

- Die **App** soll laut Hilfestellung zur Aufgabe folgende **Kernfunktionen** aufweisen:
  - Datenvalidierung (Prüfung, dass aus Gehaltsabrechnungssystem nur fest definierte Datenarten importiert werden und dass Authentifizierungsdaten bei der Eingabe nicht kompromittiert werden können)
  - Zugriffsmanagement (Prüfung der Authentifizierungsdaten und Umsetzung des Rechtekonzepts)
  - Datenverfügbarkeit (Prüfung, dass App Verbindung zum Gehaltsabrechnungssystem etabliert werden kann und dass abgerufene Gehaltsdaten lokal sicher gespeichert und dargestellt werden können)
  - Störfallmanagement (Prüfung Fail-Safe-Mechanismus)
  - Protokollierung (Zugriffsdokumentation)
  - Netzwerksicherheit (Prüfung, dass nur verschlüsselter Zugriff erfolgt)
  - Trennung der Entwicklungsumgebung von der Testumgebung und Einsatzumgebung (Übertrag von Entwicklungsdaten auf Testsysteme und von Testsysteme auf Produktivsystem via Transportsystem)
  - Schwachstellenmanagement (Monitoring der App-Sicherheit)

4.3 Privacy Impact Assessment (6)

- Ziel der PIA ist es laut Aufgabenstellung, **Vorgaben für die Durchführung der Programmierarbeiten** zu ermitteln
- Dabei ist zu betrachten, welche Auswirkung welcher App-Aspekt auf den Betroffenen haben kann hinsichtlich
  - datenschutzrechtlicher Anforderungen aus dem BDSG (d.h. weitere rechtliche Anforderungen werden für diese Aufgabe ausgeblendet)
  - der besonderen Vertrauensstellung gegenüber der verantwortlichen Stelle (auf Seiten der verantwortlichen Stelle folgen daraus Fürsorgepflichten zum Schutz der Daten)
  - der Reputation vor allem für den Fall einer Datenpanne (d.h. der unbefugten Offenbarung der Gehaltsdaten an einen Dritten, soweit daraus schwerwiegende Beeinträchtigungen für den Betroffenen resultieren können)
- In nachfolgender Tabelle sind rote Risiken inakzeptabel, orangene Risiken sind zumindest in ihrer Wirkung zu verringern, gelbe Risiken sind zu prüfen
- Zu ergreifende Maßnahmen sind in den voranstehenden Folien bereits benannt

4.3 Privacy Impact Assessment (7)

Wirkung auf Betroffenen je App-Aspekt auf Zielvorgabe	Zielvorgabe aufgrund des Datenschutzes						Zielvorgabe aufgrund Vertrauens-stellung	Zielvorgabe aufgrund betroffener Datenkategorien	
	Datensparsamkeit	Datengeheimnis	Zugangsschutz	Zugriffsschutz	Weitergabeschutz	Verfügbarkeitsschutz	Fürsorgepflicht	Vorbeugung Identitätsdiebstahl	Vorbeugung Vermögensschäden
1. Spezifikation der Anforderungen für die App (Entwicklungsumgebung)									
1.1 Nichtbeachtung des Schutzbedarfs der Nutzdaten	keine	keine	keine	keine	keine	keine	potenzieller Vertrauens-verlust	Schadens-ersatzfor-derungsrecht	potenzieller Vermögens-schaden
1.2 Nichtbeachtung des Schutzbedarfs der Quelldaten	keine	keine	keine	keine	keine	keine	fehlende Daten-integrität	keine	keine
1.3 Nichtbeachtung des Schutzbedarfs der Authentifizierungsdaten	keine	keine	unsichere Authenti-fizierung	potenzielle Datenpanne	potenzielle Datenpanne	keine	**Vertrauens-verlust**	potenzieller Vertrauens-verlust	**Vermögens-schaden**
1.4 Nichtbeachtung der Zielvorgaben	potenzielle Datenpanne	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzielle Datenpanne	potenzielle Datenpanne	potenzieller Datenverlust	potenzieller Vertrauens-verlust	Schadens-ersatzfor-derungsrecht	Schadens-ersatzfor-derungsrecht

4.3 Privacy Impact Assessment (8)

Wirkung auf Betroffenen je App-Aspekt auf Zielvorgabe	Zielvorgabe aufgrund des Datenschutzes						Zielvorgabe aufgrund Vertrauens-stellung	Zielvorgabe aufgrund betroffener Datenkategorien	
	Datensparsamkeit	Datengeheimnis	Zugangsschutz	Zugriffsschutz	Weitergabeschutz	Verfügbarkeitsschutz	Fürsorgepflicht	Vorbeugung Identitätsdiebstahl	Vorbeugung Vermögensschäden
2. Design der App (Entwicklungsumgebung)									
2.1 Unzureichende Datenvalidierung	keine	keine	fehlende Daten-integrität	fehlende Daten-integrität	unklarer Empfänger-kreis	potenzieller Datenverlust	**Vertrauens-verlust**	potenzielle Datenpanne	potenzieller Vermögens-schaden
2.2 Unzureichendes Zugriffsmanagement	keine	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzielle Datenpanne	potenzielle Datenpanne	keine	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzieller Vermögens-schaden
2.3 Unzureichende Datenverfügbarkeit	keine	keine	keine	keine	keine	potenzieller Vertrauens-verlust	**Nachweis verletzter Arbeitgeber-pflichten**	keine	keine
2.4 Unzureichendes Störfallmanagement	keine	keine	potenzielle Datenpanne	potenzielle Datenpanne	potenzielle Datenpanne	potenzieller Datenverlust	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzieller Vermögens-schaden
2.5 Unzureichende Protokollierung	keine	keine	potenzieller Vertrauens-verlust	potenzieller Vertrauens-verlust	potenzieller Vertrauens-verlust	keine	keine	keine	keine
2.6 Unzureichende Netzwerksicherheit	keine	keine	mögliche Datenpanne	mögliche Datenpanne	mögliche Datenpanne	möglicher fehlender Datenzugriff	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzieller Vermögens-schaden
2.7 Unzureichende Trennung von Entwicklungsumgebung und Testumgebung	keine	keine	potenzieller Vertrauens-verlust	mögliche Datenpanne	potenzieller Vertrauens-verlust	keine	möglicher Vertrauens-verlust	keine	keine
2.8 Unzureichendes Schwachstellenmanagement	keine	keine	keine	keine	keine	keine	Schadens-ersatzfor-derungsrecht	Schadens-ersatzfor-derungsrecht	Schadens-ersatzfor-derungsrecht

4.3 Privacy Impact Assessment (9)

Wirkung auf Betroffenen je App-Aspekt auf Zielvorgabe	Zielvorgabe aufgrund des Datenschutzes						Zielvorgabe aufgrund Vertrauens-stellung	Zielvorgabe aufgrund betroffener Datenkategorien	
	Datensparsamkeit	Datengeheimnis	Zugangsschutz	Zugriffsschutz	Weitergabeschutz	Verfügbarkeitsschutz	Fürsorgepflicht	Vorbeugung Identitätsdiebstahl	Vorbeugung Vermögensschäden
3. Implementation (Entwicklungsumgebung)									
3.1 Unzureichender Schutz der Entwicklungstools	keine	keine	keine	keine	keine	keine	möglicher Vertrauens-verlust	keine	keine
3.2 Unzureichender Schutz der Quelldaten	keine	keine	keine	keine	keine	keine	möglicher Vertrauens-verlust	keine	keine
3.3 Unzureichender Schutz der ausführbaren App-Daten	keine	keine	keine	keine	keine	keine	möglicher Vertrauens-verlust	keine	keine
4. Funktionstest (Testumgebung)									
4.1 Unvollständige Funktionstests	keine	keine	potenziell unsichere Authentifi-zierung	mögliche Datenpanne	mögliche Datenpanne	möglicher fehlender Datenzugriff	möglicher Vertrauens-verlust	keine	keine
4.2 Fehlende Tests zur Compliance mit Zielvorgaben	potenzielle Datenpanne	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzielle Datenpanne	potenzielle Datenpanne	potenzieller Datenverlust	potenzieller Vertrauens-verlust	Schadens-ersatzfor-derungsrecht	Schadens-ersatzfor-derungsrecht
4.3 Verwendung von Echtdaten für Tests	potenzielle Datenpanne	keine	keine	potenzielle Datenpanne	keine	keine	potenzieller Vertrauens-verlust	keine	keine
4.4 Unzureichender Schutz der Testdaten	keine	keine	keine	keine	keine	keine	möglicher Vertrauens-verlust	keine	keine

4.3 Privacy Impact Assessment (10)

Wirkung auf Betroffenen je App-Aspekt auf Zielvorgabe	Zielvorgabe aufgrund des Datenschutzes						Zielvorgabe aufgrund Vertrauens-stellung	Zielvorgabe aufgrund betroffener Datenkategorien	
	Datensparsamkeit	Datengeheimnis	Zugangsschutz	Zugriffsschutz	Weitergabeschutz	Verfügbarkeitsschutz	Fürsorgepflicht	Vorbeugung Identitätsdiebstahl	Vorbeugung Vermögensschäden
5. Einsatz der App (Einsatzumgebung)									
5.1 Unzureichende Absicherung der Schnittstellen zum Abrechnungssystem	potenzielle Datenpanne	möglicher Vertrauens-verlust	potenzielle Datenpanne	potenzielle Datenpanne	potenzielle Datenpanne	potenzieller Datenverlust	potenzieller Vertrauens-verlust	möglicher Vertrauens-verlust	Schadens-ersatzfor-derungsrecht
5.2 Unzureichende Trennung von Testumgebung und Einsatzumgebung	keine	keine	potenzieller Vertrauens-verlust	mögliche Datenpanne	potenzieller Vertrauens-verlust	keine	möglicher Vertrauens-verlust	keine	keine
5.3 Unzureichender Schutz der Authentifizierungsdaten	keine	keine	unsichere Authenti-fizierung	**Datenpanne**	**Datenpanne**	keine	**Vertrauens-verlust**	möglicher Vertrauens-verlust	**Vermögens-schaden**
5.4 Unzureichender Schutz der Nutzdaten	potenzielle Datenpanne	keine	potenzielle Datenpanne	potenzielle Datenpanne	potenzielle Datenpanne	keine	potenzieller Vertrauens-verlust	potenzielle Datenpanne	potenzieller Vermögens-schaden
5.5 Unzureichende Verschlüsselung	keine	keine	keine	mögliche Datenpanne	mögliche Datenpanne	keine	möglicher Vertrauens-verlust	möglicher Vertrauens-verlust	Schadens-ersatzfor-derungsrecht
5.6 Unzureichender Schutz lokal gespeicherter Daten	keine	keine	keine	mögliche Datenpanne	potenzielle Datenpanne	möglicher fehlender Datenzugriff	möglicher Vertrauens-verlust	keine	keine

4.4 Voice over IP

Aufgabe:

- Ein Unternehmen möchte seine bisherige analoge Telefontechnik mit einer TK-Anlage ersetzen, die Voice over IP einsetzt. Dabei sollen Einzelverbindungs-nachweise zu den einzelnen Telefongesprächen zu Zwecken einer sachgerechten Kostenstellenrechnung aufgezeichnet werden. Das Unternehmen verfügt über einen Betriebsrat. Eine private Nutzung der Telefonanlage ist gestattet, sofern die Mitarbeiter hierzu eine spezifische Vorwahl wählen. Sobald diese Vorwahl gewählt wird, erhalten die Telefonstelleninhaber eine Rechnung, die monatlich vom Gehalt abgezogen wird. Wie muss das Unternehmen vorgehen, damit das zulässig ist? Begründen Sie Ihre Antwort unter Einbeziehung des BetrVG [in Aufgabe leider fehlerhaft BVerfG genannt!], TKG und BDSG!

4.4 Voice over IP (1)

- Voice over IP = Telefonie vermittels des Internet Protocols
  → Übertragung der Sprachdaten via Internet
  → Vertraulichkeit des Wortes nur gesichert, wenn Sprachdaten verschlüsselt werden
- Für Aufzeichnung der Einzelverbindungsnachweise ist § 99 TKG einschlägig!
  → Unternehmen ist Teilnehmer im Sinne von § 99 Abs. 1 TKG
  → Teilnehmer entscheidet, ob Rufnummern unter Kürzung der letzten 3 Stellen mitgeteilt werden
  → Teilnehmer muss erklären, dass er seine Mitarbeiter über Aufzeichnung informiert hat (und muss folglich seine Mitarbeiter darüber informieren)
  → Teilnehmer muss Betriebsrat beteiligen (Unterrichtung nach §§ 80 Abs. 2 & 90 Abs. 1 Nr. 2 BetrVG, Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG)
  → Diensteanbieter ist hier der Internet-Provider
- Aufgrund der Gestattung zur Privatnutzung unterliegen die Sprachdaten dem Fernmeldegeheimnis und dürfen nicht ohne Einwilligung der Nutzer (= Mitarbeiter) aufgezeichnet werden (wegen § 88 Abs. 3 TKG)

4.4 Voice over IP (2)

- I.d.R. wird Einführung von Voice over IP in diesem Fall mittels einer Betriebsvereinbarung nach § 77 Abs. 2 BetrVG einvernehmlich geregelt
  → Betriebsrat willigt kollektivrechtlich für Mitarbeiter in Aufzeichnung ein
  → Da Betriebsvereinbarung ebenfalls allen Mitarbeitern bekannt zu machen ist, kann Information der Mitarbeiter auch vermittels der Betriebsvereinbarung erfolgen
- I.d.R. wird in diesem Zusammenhang festgelegt, dass Umfang der Telefonie nur zur Abrechnung der privaten Telefonate erfolgt
  → Da spezifische Vorwahl zu wählen ist, werden andere Daten nur vorübergehend zur Missbrauchskontrolle gespeichert (versehentliches oder absichtliches Nichteingeben der kostenpflichtigen Vorwahl)
  → Stichprobenkontrollen in Betriebsvereinbarung festlegen
- Restriktiv vergebene Zugriffsrechte, damit nur Befugte Verkehrsdaten nach § 96 TKG einsehen können

4.4 Konzerndatenschutz

Aufgabe:

- Ein Konzern möchte seine Ressourcen effizienter einsetzen und gliedert Funktionseinheiten in eine zentrale Servicegesellschaft aus, die für alle Unternehmen im Konzern einerseits IT-Dienstleistungen und andererseits HR-Dienstleistungen erbringt. Diese Funktionen werden aus den einzelnen Gesellschaften entfernt und in der neu gegründeten Servicegesellschaft gebündelt. Die Konzernholding hält alle Gesellschaftsanteile aller Tochtergesellschaften. Der Konzern verfügt über einen Betriebsrat. Dieser hat der Ausgliederung nur unter der Bedingung zugestimmt, dass die Serviceerbringung via Auftragsdatenverarbeitung erbracht wird, um weiterhin vollen Einfluss geltend machen zu können. Welche Regelungen sind zu treffen, damit diese Voraussetzung erfüllt ist? Begründen Sie Ihre Antwort!

4.5 Konzerndatenschutz (1)

- Auslagerung in zentrale Servicegesellschaft stellt Betriebsänderung im Sinne von § 111 BetrVG dar
- Vereinbarter Interessenausgleich nach § 112 Abs. 1 BetrVG schriftlich festzuhalten
- Für Auftragsdatenverarbeitung sind die Auflagen aus § 11 Abs. 2 BDSG zu beachten, d.h. die zentral erbrachten Services müssen im Einzelnen zwischen den jeweiligen Auftraggebern und der zentralen Servicegesellschaft (Auftragnehmer) schriftlich vereinbart werden (i.d.R. im Rahmen eines Kooperationsvertrags)
- Im vorliegenden Fall sollen neben den IT-Dienstleistungen auch HR-Dienstleistungen durch die zentrale Servicegesellschaft erbracht werden
  → Mandatentrennung einrichten
  → Aufgrund üblicher Informationspflichten gegenüber Konzernholding, bedarf die Weitergabe und Aggregation entsprechender Daten der ausdrücklichen Festlegung im Auftrag
  → Zu erbringende Services sind detailliert zu beschreiben

4.5 Konzerndatenschutz (2)

- Für Auftragnehmer gilt außerdem ausdrücklich § 11 Abs. 4 BDSG
- Aufgrund der zu erbringenden IT-Dienstleistungen ist zudem der Zugriff auf wietere personenbezogene Daten des jeweiligen Auftraggebers nicht ausschließbar
- Die jeweiligen Auftraggeber bleiben weiterhin voll verantwortlich für ausgelagerte Dienstleistungen