Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2014:
Mitarbeiterdatenschutz (3)

4.1 Intranet

Aufgabe:

- Ein Unternehmen möchte im Intranet ein innerbetriebliches Mitteilungsforum einrichten. Über dieses Forum sollen den Mitarbeitern zentrale Informationen über betriebliche Themen mitgeteilt werden (inkl. betriebliche Handbücher, Wikis und Bilder über Betriebsfeste). Für jeden Mitarbeiter wird automatisch ein entsprechender Account angelegt. Wenn eine neue Verhaltensrichtlinie eingeführt wird, erfolgt eine automatische Aufforderung per Mail an die Mitarbeiter, diese Richtlinie anzuklicken. Das wird mittels einer Software mit Newsletterfunktionalität auch überprüft, da die Kenntnis der Richtlinie im Arbeitsvertrag zwingend vorgeschrieben ist. Welche Anforderungen aus dem TMG und dem BDSG sind für die Einrichtung dieses Mitteilungsforum zu beachten?

Anmerkung: Im Gegensatz zum Internet ist das Intranet nur betriebsöffentlich.

4.1 Intranet (1)

- Intranet = betriebsöffentliche Plattform → keine allgemein zugängliche Quelle im Sinne von § 28 Abs. 1 Nr. 3 BDSG
- Zu den „betrieblichen Mitteilungen“ zählen u.a. Bilder über Betriebsfeste, die ggf. nur mit Zustimmung der Abgebildeten im Intranet veröffentlicht werden dürfen
→ Anforderung: § 4a BDSG für Einwilligung (damit keine Vorabkontrolle nötig!)
- Im Intranet sollen Verhaltensrichtlinien verbindlich eingeführt werden unter Ausnutzung des Newslettermechanismus (entspricht Verwendung von Nutzungsdaten im Sinne des TMG). Allerdings wird laut Aufgabenstellung das Intranet offenbar nur für berufliche und dienstliche Zwecke verwendet, weshalb der 4. Abschnitt des TMG nach § 11 Abs. 1 Nr. 1 TMG nicht zur Anwendung kommt.
- Für das Intranet sind demnach nur die allgemeinen Bestimmungen und die Bestimmungen über nicht-öffentliche Stellen aus dem BDSG einschlägig
- Zulässigkeit bemisst sich nach § 4 Abs. 1 BDSG
→ § 28 Abs. 1 Nr. 2 BDSG (für generelle Datenverwendung)
→ § 32 Abs. 1 BDSG (für Verhaltensrichtlinien, da Bestandteil Arbeitsvertrag)

4.1 Intranet (2)

- Ansonsten gelten die üblichen Anforderungen:
 - Verpflichtung auf das Datengeheimnis (§ 5 BDSG)
 - Gewährleistung der Betroffenenrechte (§ 6 Abs. 1 BDSG & §§ 34 & 35 BDSG)
 - Angemessene technische & organisatorische Maßnahmen (§ 9 BDSG)

4.2 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!

4.2 Voice over IP (1)

- Voice over IP = Telefonie vermittelt des Internet Protocols
 - Übertragung der Sprachdaten via Internet
 - Vertraulichkeit des Wortes nur gesichert, wenn Sprachdaten verschlüsselt werden
- Für Aufzeichnung der Einzelverbindungs nachweise 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)

4.2 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

4.3 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?

4.3 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

4.3 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)

4.4 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!

4.4 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

4.4 Konzerndatenschutz (2)

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

4.5 Bestimmung des Datenschutzniveaus

Aufgabe:

- Anhand welcher Prüfkriterien, die sich aus dem BDSG ablesen lassen, kann hinsichtlich des Mitarbeiterdatenschutzes das Datenschutzniveau eines Unternehmens beurteilt werden?

4.5 Bestimmung des Datenschutzniveaus (1)

- Mitarbeiter = Betroffener innerhalb des Unternehmens
- Verzeichnisse mit Angaben aus § 4e BDSG vorhanden?
- Beschäftigter ausreichend über alle im Verzeichnis aufgeführten Verfahren informiert?
- Sofern Verfahren auf der Grundlage einer Einwilligungserklärung durchgeführt wird, wurde der Beschäftigte über alle vorgesehenen Zwecke und über sein Widerrufsrecht (z.B. bei Ablage von Betriebsfestbildern) informiert?
- Hat sich das Unternehmen bei den direkt beim Betroffenen erhobenen Daten auf erforderliche Daten beschränkt?
- Hat das Unternehmen einen Datenschutzbeauftragten bestellt?
- Kann der Datenschutzbeauftragte ausreichend leicht vom Betroffenen kontaktiert werden?
- Wird der Schutz der Betroffenenidentität bei Datenschutzanfragen gewahrt?
- Wird dem Betroffenen auf Anfrage mitgeteilt, auf welcher Rechtsgrundlage seine Daten bei einzelnen Verfahren automatisiert verarbeitet werden?

4.5 Bestimmung des Datenschutzniveaus (2)

- Werden die Betroffenenrechte angemessen rasch umgesetzt?
- Wurde der Beschäftigte ausreichend über datenschutzrechtliche Bestimmungen (z.B. im Rahmen seiner EDV-Einführung) unterwiesen?
- Sind die technischen und organisatorischen Maßnahmen zu den Verfahren, die der Beschäftigte selbst bearbeitet, aus seiner Sicht ausreichend?
- Wird dem Beschäftigten sein Einsichtsrecht in seine Personalakte gewährt?
- Ist seine Personalakte vollständig (keine Nebenakten) und korrekt (aktuell)?
- Befinden sich in der Personalakte keine unnötigen Unterlagen?
- Sofern eine Videoüberwachung besteht: Besteht eine ausreichende Kennzeichnung zur bestehenden Videoüberwachung?
- Genügt der Umfang der bereitgestellten Betroffenenendaten im Intranet dem Grundsatz der Datensparsamkeit nach § 3a BDSG?
- Soweit ein Betriebsrat besteht: Sind in den einzelnen Betriebsvereinbarungen ausdrücklich Regelungen zum Datenschutz integriert?