Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2015:
Mitarbeiterdatenschutz (4)

5.1 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.

5.1 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 Newslettermechanismusses (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)

5.1 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)

5.2 Aufgaben Mitarbeiterdatenschutz I

Aufgabe:

- Bei einem Unternehmen ist unter Verwendung des **RACI-Modells** festzulegen, welche Stelle welche Aufgabe im Rahmen der Gewährleistung des Mitarbeiterdatenschutzes zu erfüllen hat. Erstellen Sie eine Übersicht, in der Sie typische Aufgaben zur Gewährleistung des Mitarbeiterdatenschutzes folgenden Stellen zuweisen:
  - Geschäftsführer (in der Funktion als Vertreter der verantwortlichen Stelle)
  - HR-Leiter (als Verantwortlicher für alle Aufgaben im Bereich HR)
  - IT-Leiter (als Verantwortlicher für alle Aufgaben mit IT-Bezug)
  - Datenschutzbeauftragter
  - HR-Mitarbeiter (ausführende Stelle im Bereich HR)
  - Systemadministrator (ausführende Stelle im Bereich IT)

  Berücksichtigen Sie in Ihrer Lösung nur folgende Verfahren:
  - Personalaktenführung
  - Arbeitszeitüberwachung
  - Elektronische Kommunikation

5.2 Aufgaben Mitarbeiterdatenschutz II

Aufgabe:

- Konzentrieren Sie sich dabei auf das Wesentliche und gehen Sie bei Ihrer Lösung davon aus, dass nur die HR-Verfahren hinsichtlich des IT-Bereichs betrachtet werden (die IT ist insoweit betroffene als auch ausführende Stelle, prozessverantwortlich ist aber HR). Beachten Sie bei Ihrer Lösung, dass niemand eine Aufgabe umzusetzen hat, der diese Aufgabe zugleich zu genehmigen hat.
  Hinweis:
  *Beim **RACI-Modell** gibt es vier Rollen, nämlich*
  ***R = Responsible** → Umsetzung einer Aufgabe*
  ***A = Accountable** → Genehmigung einer Aufgabe*
  ***C = Consulted** → Anhörungsinstanz bei einer Aufgabe*
  ***I = Informed** → Mitteilungsempfangsinstanz bei einer Aufgabe*

5.2 Aufgaben Mitarbeiterdatenschutz (1)

Datenschutz bei der Personalaktenführung	GF	HR-Leiter	IT-Leiter	DSB	HR-MA	Sysadm.
Überführung der Bewerbungsunterlagen in die Personalakte	I	A	C *		R	
Geeignete Aufbewahrung der Personalakte	I	A		C	R	
Akkurate und aktuelle Führung der Personalakte		A		C	R	
Dokumentation zur Einsicht in die Personalakte		A		C	R	
Entfernung zu löschender Unterlagen aus der Personalakte (z.B. von Abmahnungen)		A		C	R	
Aussonderung der Personalakte ausgeschiedener Mitarbeiter ins Archiv	I	A	I *	C	R	

Datenschutz bei der Arbeitszeitüberwachung	GF	HR-Leiter	IT-Leiter	DSB	HR-MA	Sysadm.
Anlage des Referenzmodells laut Anstellungsvertrag	I	A	C *		R	
Aufzeichnung der Arbeitszeitdaten		C	A *		I	R *
Geschützte Speicherung der Aufzeichnungsdaten		A	R	C	I	I
Kontrolle der Aufzeichnungsdaten auf Einhaltung des Referenzmodells		A	I *	C	R	
Löschen der Aufzeichnungsdaten nach Ablauf der Aufbewahrungsfrist		A	C	C	R	

5.2 Aufgaben Mitarbeiterdatenschutz (2)

Datenschutz bei der Elektronischen Kommunikation	GF	HR-Leiter	IT-Leiter	DSB	HR-MA	Sysadm.
Einrichtung der Kommunikationsdienste für neue Mitarbeiter	I	C	A			R
Sicherer Betrieb der Kommunikationsdienste	C		A	C		R
GoBD-konforme Archivierung elektronischer Kommunikation	C		A	C		R
Einsicht in Kommunikationsdaten bei betrieblicher Notwendigkeit und Abwesenheit des Mitarbeiters	A		R	C		I *
Löschen der Kommunikationsdaten nach Ablauf der Aufbewahrungsfrist	C		A	C		R

5.3 Datenschutzmanagement

Aufgabe:

- Welche Prozesse hat ein Unternehmen zum Datenschutzmanagement aufgrund der datenschutzrechtlichen Bestimmungen aus BDSG, BetrVG & TMG umzusetzen?
  Hinweis: Orientieren Sie sich dabei an den Aufgaben, die der Datenschutzbeauftragte in Zusammenarbeit mit anderen Stellen im Unternehmen im Zusammenhang mit dem Mitarbeiterdatenschutz zu erfüllen hat.

5.3 Datenschutzmanagement (1)

Prozesse zum Management des Mitarbeiterdatenschutzes aus dem **BDSG**:

Alle nachstehenden Angaben sind nicht nur auf Mitarbeiterdatenschutz beschränkt.

- **Bestellung eines Datenschutzbeauftragten**, soweit die Bestellung nicht vorgeschrieben ist (§ 4f Abs. 1 BDSG), sonst nimmt der Leiter der nicht-öffentlichen Stelle dessen Aufgaben wahr (§ 4g Abs. 2a BDSG)
- **Vorabkontrolle** von automatisierten Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen können (§ 4d Abs. 6 BDSG i.V.m. § 4d Abs. 5 BDSG)
  → neue Verfahren beim Datenschutzbeauftragten anmelden!
  → hierzu Übersicht nach § 4g Abs. 2 Satz 1 vorlegen (= öffentliches Verfahrensverzeichnis plus allgemeine Beschreibung der Schutzvorkehrungen plus Liste über zugriffsbefugte Personen)
  → Angaben über Datenfluss und Zugriffsrollenkonzept
- **Regelkontrolle zur Überwachung** der ordnungsgemäßen Anwendung der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen (§ 4g Abs. 1 Satz 4 Nr. 1 BDSG)
  → hierzu rechtzeitig über Vorhaben der automatisierten Verarbeitung personenbezogener Daten zu unterrichten!

5.3 Datenschutzmanagement (2)

Prozesse zum Management des Mitarbeiterdatenschutzes aus dem **BDSG**: 1. Forts.

- **Vertrautmachen der** bei der Verarbeitung personenbezogener Daten **tätigen Personen mit datenschutzrechtlichen Vorschriften** durch geeignete Maßnahmen (§ 4g Abs. 1 Satz 4 Nr. 2 BDSG):
  → Schulungen
  → Informationsschriften / Merkblätter
  → Belehrungen
  → insbesondere bei der Verpflichtung auf das Datengeheimnis nach § 5 BDSG
- **Bekanntgabe des öffentlichen Verfahrensverzeichnisses** (§ 4g Abs. 2 Satz 2 BDSG)
- **Unterstützung** des Datenschutzbeauftragten bei der Aufrechterhaltung seiner Fachkunde durch Teilnahme an Fort- und Weiterbildungsveranstaltungen (§ 4f Abs. 3 Satz 7 BDSG)
- **Unterstützung** des Datenschutzbeauftragten durch erforderliches Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel (§ 4f Abs. 5 Satz 1 BDSG)
- **Bearbeitung von Betroffenenanliegen** unter Wahrung der Verschwiegenheit über deren Identität (§ 4f Abs. 5 Satz 2 BDSG i.V.m. § 4f Abs. 4 BDSG)

5.3 Datenschutzmanagement (3)

Prozesse zum Management des Mitarbeiterdatenschutzes aus dem **BDSG**: 2. Forts.

- **Hinwirken auf** die Beachtung der den Umständen des Falles gebotenen **Sorgfalt** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 7 Satz 2 BDSG)
- **Hinwirken auf** das Treffen angemessener **technischer und organisatorischer Maßnahmen** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 9 BDSG)
- **Hinwirken auf** die Auswahl geeigneter **Auftragnehmer** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 11 Abs. 2 BDSG)
- **Hinwirken auf** die korrekte Durchführung erforderlicher **Abwägungen** (§ 4g Abs. 1 Satz 1 BDSG i.V.m.:
  - § 6b Abs. 1 BDSG bei der Videoüberwachung
  - § 10 Abs. 1 BDSG bei Abrufverfahren
  - § 28 Abs. 1 Satz 1 Nr. 2 BDSG zur Erfüllung eigener Geschäftszwecke
  - § 28 Abs. 2 Satz 1 Nr. 2 BDSG zur Erfüllung anderer Zwecke
  - § 28 Abs. 6 Nr. 3 & 4 BDSG beim Umgang mit besonderen Arten personenbezogener Daten
  - § 29 Abs. 1 Nr. 1 & 2 BDSG zur geschäftsmäßigen Übermittlung
  - § 30 Abs. 2 BDSG zur Übermittlung veränderter Daten)

5.3 Datenschutzmanagement (4)

Prozesse zum Management des Mitarbeiterdatenschutzes aus dem **BDSG**: 3. Forts.

- **Hinwirken auf** die Einhaltung der **Betroffenenrechte** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. §§ 33 – 35 BDSG)
- **Hinwirken auf** einen korrekten **Ablauf bei Eintritt einer Datenpanne** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 42a BDSG)

Prozesse zum Management des Mitarbeiterdatenschutzes aus dem **TMG**:

- **Hinwirken auf** die Einhaltung der strengen **Zweckbindung bei Einsatz von Telemedien** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 12 TMG)
- **Hinwirken auf** die korrekte Darstellung der **Datenschutzerklärung** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 13 Abs. 1 TMG)
- **Hinwirken auf die spezifischen technischen und organisatorischen Maßnahmen** aus dem Telemedienrecht (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 13 Abs. 4 TMG)
- **Hinwirken auf** die Erfüllung des **Auskunftsrechts der Nutzer** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 13 Abs. 7 TMG)
- **Hinwirken auf** einen korrekten **Ablauf bei Eintritt einer Datenpanne** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 15a TMG)

5.3 Datenschutzmanagement (5)

Prozesse zum Management des Mitarbeiterdatenschutzes aus dem **BetrVG**:

- **Hinwirken auf** die Einhaltung mitbestimmungsrechtlicher Vorgaben bei Verfahren zur **Leistungs- und/oder Verhaltenskontrolle** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. § 87 Abs. 1 Nr. 1 & 6 BetrVG)
  → i.d.R. im Rahmen der Vorabkontrolle, da Mitbestimmungsrecht hier vorrangiges Recht ist
- **Hinwirken auf** die Beteiligung des Betriebsrats bei **personellen Einzelmaßnahmen** (§ 4g Abs. 1 Satz 1 BDSG i.V.m. §§ 99 Abs. 1 und 102 Abs. 1 BetrVG)
- **Hinwirken auf** die rechtzeitige Information des Betriebsrats (§ 4g Abs. 1 Satz 1 BDSG i.V.m. §§ 80 Abs. 2 und 90 Abs. 1 BetrVG)

Anmerkung: Die mitbestimmungsrechtlichen Aufgaben haben nur einen mittelbaren Bezug zum Datenschutz, der auf § 75 Abs. 2 BetrVG basiert.

5.4 Protokollierung von Netzwerktraffic

Aufgabe:

- Welche Vorschriften aus BDSG & TMG sind zu beachten, wenn der Traffic auf dem Netzwerk protokolliert werden soll? Geben Sie hierzu die präzise Rechtsquelle an!

5.4 Protokollierung von Netzwerktraffic (1)

Netzwerktraffic = Transfer von Datenpaketen über das Netzwerkmedium

- → Network Layer (Schicht 3 im ISO/OSI-Referenzmodell)
- → Im Network Layer wird insbesondere das Internet Protocol angewandt
- → IP-Adressen sind als personenbezogene Daten anzusehen
- → Netzwerktraffic betrifft insbesondere Datenverkehr mit Dritten und fällt daher nicht unter die Ausnahmebestände aus § 11 Abs. 1 TMG!
- → TMG hier daher einschlägig, soweit Telemediendienste betroffen sind: das ist für den Mail-Dienst und für den Web-Dienst der Fall
- → Netzwerktraffic wird i.d.R. nur aufgezeichnet, um den ordnungsgemäßen Betrieb einer Datenverarbeitung feststellen zu können
- → **Maßgebliche Rechtsgrundlage für die Protokollierung von Netzwerktraffic ist daher § 31 BDSG!**
- → Nach § 15 Abs. 1 Satz 1 TMG darf ein Diensteanbieter personenbezogene Nutzerdaten nur erheben und verwenden, soweit dies für die Inanspruchnahme der Telemedien erforderlich ist

5.4 Protokollierung von Netzwerktraffic (2)

1. Fortsetzung über weitere Rechtsgrundlagen:

- § 3a BDSG: keine oder so wenig personenbezogene Daten wie möglich aufzeichnen
- § 4 Abs. 1 BDSG bzw. § 12 Abs. 1 TMG: Zulässigkeit nur aufgrund Rechtsvorschrift (hier: § 31 BDSG) oder Einwilligung
- § 4a Abs. 1 BDSG & § 28 Abs. 3a BDSG bzw. § 13 Abs. 2 TMG: Einwilligung muss auf infor-mierter Basis freiwillig & bewusst erfolgen und muss nachweisbar sein
  (Anmerkung: Einwilligung wird hier i.d.R. nicht relevant sein!)
- § 4g Abs. 1 BDSG: Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme obliegt dem zuständigen Datenschutzbeauftragten
- § 5 BDSG: eine unbefugte Verarbeitung personenbezogener Daten ist verboten; im erlaubten Fall Verpflichtung auf Datengeheimnis
- § 6 Abs. 1 BDSG bzw. § 13 Abs. 7 TMG: Auskunftsrecht des Betroffenen bzw. Nutzers

5.4 Protokollierung von Netzwerktraffic (3)

2. Fortsetzung über weitere Rechtsgrundlagen:

- § 6 Abs. 1 BDSG bzw. § 35 Abs. 2 Nr. 3 BDSG: Betroffener hat auch Recht auf Löschung
- § 13 Abs. 4 Satz 2 TMG: Diensteanbieter hat unverzügliche Löschung sicherzustellen, soweit nicht Aufbewahrungsfristen entgegenstehen (Anmerkung: Der Gesetzgeber hat es bisher leider versäumt, für die Aufbewahrung von Protokolldaten gesetzliche Vorschriften zu erlassen)
- § 28 Abs. 1 Nr. 2 BDSG: zur Erfüllung eigener Geschäftszwecke ist Datenverarbeitung zur Wahrung berechtigter Interessen zulässig, sofern kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffenen diesem entgegenstehen
- § 28 Abs. 1 Satz 2 BDSG: Zweck der Datenverarbeitung ist bei der Erhebung konkret festzulegen
- § 31 BDSG: Protokolldaten dürfen nur zur Datenschutzkontrolle, Datensicherung bzw. Sicherstellung des ordnungsgemäßen Betriebs der DV-Anlage verwendet werden

5.5 Bestimmung des Datenschutzniveaus

Aufgabe:

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

5.5 Bestimmung des Datenschutzniveaus (1)

- Mitarbeiter = Betroffener innerhalb des Unternehmens
- Verfahrensverzeichnis mit Angaben aus § 4e BDSG vorhanden?
- Beschäftigter ausreichend über alle im Verfahrensverzeichnis 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?

5.5 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 Betroffenendaten im Intranet dem Grundsatz der Datensparsamkeit nach § 3a BDSG?
- Soweit ein Betriebsrat besteht: Sind in den einzelnen Betriebsvereinbarungen ausdrücklich Regelungen zum Datenschutz integriert?