Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2017:
Mitarbeiterdatenschutz (3)

5.1 Protokollierung von Netzwerktraffic

Aufgabe:

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

5.1 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 personenbezogene Daten (Online-Kennung)
- → 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 Art. 6 Abs. 1 lit. f EU-DSGVO! (vgl. ErwG 49)**
- → *Einschränkung aus § 15 Abs. 1 Satz 1 TMG nach EuGH-Urteil vom 19.10.2016 (Rechtsache C-582/14) nichtig → Nutzungsdaten dürfen zu Zwecken der Gewährleistung der Funktionsfähigkeit genutzt werden!*

5.1 Protokollierung von Netzwerktraffic (2)

1. Fortsetzung über weitere Rechtsgrundlagen:

- Art. 5 Abs. 1 lit. a EU-DSGVO: Verarbeitung muss dem Grundsatz von Treu und Glauben genügen und für den Betroffenen transparent sein
  → Information des Betroffenen nach Art. 14 EU-DSGVO
  → *kann auch in Form einer BV erfolgen, falls BR vorhanden*
- Art. 5 Abs. 1 lit. b EU-DSGVO: Zwecke müssen festgelegt werden
  → Gewährleistung der Funktionsfähigkeit zulässig (Art. 6 Abs. 1 lit. f EU-DSGVO)
- Art. 5 Abs. 1 lit. c EU-DSGVO: nur zweckerhebliche personenbezogene Daten aufzeichnen
  → IP-Adressen nur aufzeichnen, wo z.B. zur Störungserkennung nötig
  → Pseudonymisierung nach Art. 25 Abs. 1 EU-DSGVO
  (*Anmerkung: IP-Adressen gewährleisten eben nicht schon per se Erfüllung von Art. 4 Nr. 5 EU-DSGVO*)
- Art. 39 Abs. 1 lit. b EU-DSGVO: Überwachung der Einhaltung der EU-DSGVO durch Datenschutzbeauftragten

5.1 Protokollierung von Netzwerktraffic (3)

2. Fortsetzung über weitere Rechtsgrundlagen:

- Art. 15 EU-DSGVO bzw. § 13 Abs. 7 TMG: Auskunftsrecht des Betroffenen bzw. Nutzers
- Art. 17 EU-DSGVO: Betroffener hat Recht auf Löschung, sobald Personenbezug nicht mehr nötig (Art. 17 Abs. 1 lit. a EU-DSGVO) und Daten nicht mehr zur Geltendmachung von Rechtsansprüchen, z.B. zur Verfolgung von Angriffen, nötig (Art. 17 Abs. 1 lit. e EU-DSGVO)
- § 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*)

5.2 Zentrale Kalenderfunktion

Aufgabe:

- Ein Unternehmen möchte die Termine ihrer Mitarbeiter, die mit der agilen Programmierung beschäftigt sind und sich regelmäßig in Teams koordinieren müssen, in seinem Mailsystem pflegen, welches über eine Funktion zur Terminverwaltung aller Mitarbeiter verfügt. Dabei sollen Abwesenheiten unter Angabe des Grundes (Urlaub, Fortbildung, Dienstreise, Krankheit) eingetragen werden. Die Mitarbeiter sollen hierzu in eine Nutzungsordnung einwilligen. Ist das zulässig? Begründen Sie Ihre Antwort!

5.2 Zentrale Kalenderfunktion (1)

- Bei agiler Programmierung (z.B. nach Scrum) ist es tatsächlich erforderlich, dass sich Teams untereinander koordinieren, auch hinsichtlich der Zeiten (kurze Umsetzungszyklen, funktional differenziertes Team, Team organisiert sich selbst)
- Insoweit ist die Nutzung einer zentralen Kalenderfunktion, welche von allen einschlägigen Mailsystemen zur Verfügung gestellt werden, zur terminlichen Koordination zweckmäßig
- In diesen Kalendern sind zwingend geplante Abwesenheiten einzutragen, wie Urlaub, Fortbildung und Dienstreisen, da zu diesen Zeiten ein Team-Mitglied nicht für Abstimmungsrunden zur Verfügung steht
  → Umsetzung des Anstellungsvertrags der Programmierer nach Art. 6 Abs. 1 lit. b EU-DSGVO
  → Zugriff auf Abwesenheitszeiten dürfen aber nur die Teammitglieder (und der Scrum-Master plus Produkt Owner sowie der disziplinarische Dienstvorgesetzte) haben
- Ungeplante Abwesenheitszeiten wie z.B. Krankheit und Unfall haben zwar ebenfalls einen Einfluss auf die kurzfristige Terminkoordination, sind aber als „Profiling“ im Sinne von Art. 4 Nr. 4 EU-DSGVO anzusehen und ggf. auch als „Gesundheitsdaten“ im Sinne von Art. 4 Nr. 15 EU-DSGVO

5.2 Zentrale Kalenderfunktion (2)

- Die Angabe des Grundes für die kurzfristige Abwesenheit ist für die Terminkoordination nicht erforderlich
  → Aufgrund des Grundsatzes der Datenminimierung ist die Angabe „Krankheit“ nicht erforderlich und damit in der zentralen Kalenderfunktion nicht zulässig (Art. 5 Abs. 1 lit. c EU-DSGVO)
  → Um dieses Datum dennoch so eintragen zu können, wäre nötig:
    ° Einwilligung der Betroffenen nach Art. 9 Abs. 2 lit. a EU-DSGVO (allerdings mit fragwürdiger Freiwilligkeit!)
    ° Betriebsvereinbarung nach § 77 Abs. 4 BetrVG (= Kollektivvereinbarung nach Art. 9 Abs. 2 lit. b EU-DSGVO)
- Nach Aufgabenstellung ist hierfür eine Einwilligung in eine Nutzungsordnung geplant, d.h., um die zentrale Kalenderfunktion für die Terminkoordination nutzen zu können, sollen die Programmierer darin einwilligen, dass die Abwesenheitsgründe darin erfasst werden
  → Nutzungsordnung müsste nach Art. 7 Abs. 3 EU-DSGVO jederzeit für die Betroffenen widerrufbar sein
  → Widerruf der Nutzungsordnung führt dazu, dass die Arbeitsfähigkeit des Programmierteams gefährdet ist
  → Einwilligung untauglich! → Fragwürdig & untauglich → **Unzulässig**!

5.3 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 des Verantwortlichen)
  ° HR-Leiter (als Aufgabenverantwortlicher im Bereich HR)
  ° IT-Leiter (als Aufgabenverantwortlicher im Bereich IT)
  ° 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

5.3 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*

5.3 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	

5.3 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

* = Nur soweit Mitarbeiter der IT betroffen

5.4 Datenschutzmanagement

Aufgabe:

- Welche Prozesse hat ein Unternehmen zum Datenschutzmanagement aufgrund der datenschutzrechtlichen Bestimmungen aus EU-DSGVO, 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.

5.4 Datenschutzmanagement (1)

Prozesse zum Management des Mitarbeiterdatenschutzes nach **EU-DSGVO**:

Alle nachstehenden Angaben sind nicht nur auf Mitarbeiterdatenschutz beschränkt.

- **Führung des Verzeichnisses von Verarbeitungstätigkeiten** nach Art. 30 Abs. 1 EU-DSGVO durch Verantwortliche bzw. nach Art. 30 Abs. 2 EU-DSGVO durch Auftragsverarbeiter
- **Benennung eines Datenschutzbeauftragten** nach Art. 37 Abs. 1 EU-DSGVO
- **Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten** nach Art. 37 Abs. 7 EU-DSGVO
- **Datenschutz-Folgenabschätzung** von Verarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aufweisen können nach Art. 35 Abs. 1 EU-DSGVO unter Beteiligung des Datenschutzbeauftragten nach Art. 35 Abs. 2 EU-DSGVO
  → neue Verfahren beim Datenschutzbeauftragten anmelden!
  → Angaben aus Verzeichnis von Verarbeitungstätigkeiten melden (inkl. geplanter Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO)
  → Angaben über verfolgte berechtigte Interessen, Datenfluss und Zugriffsrollen
  → Rat des Datenschutzbeauftragten einholen! (Art. 39 Abs. 1 lit. c EU-DSGVO)
  → Bewertung Notwendigkeit, Verhältnismäßigkeit & Risiken

5.4 Datenschutzmanagement (2)

Prozesse zum Management des Mitarbeiterdatenschutzes n. **EU-DSGVO**: 1. Forts.

- **Regelkontrolle zur Überwachung** der Einhaltung datenschutzrechtlicher Vorschriften nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Datenschutzbeauftragten rechtzeitig über bestehende & geplante Verarbeitung unterrichten nach Art. 38 Abs. 1 EU-DSGVO!
  → i.d.R. durch Verzeichnis von Verarbeitungstätigkeiten
  → unter Berücksichtigung der Risiken nach Art. 39 Abs. 2 EU-DSGVO
- **Unterrichtung und Beratung der** bei der Verarbeitung personenbezogener Daten **tätigen Personen über ihre datenschutzrechtlichen Pflichten** nach Art. 39 Abs. 1 lit. a EU-DSGVO:
  → Schulungen & Sensibilisierungen nach Art. 39 Abs. 1 lit. b EU-DSGVO
  → Informationsschriften / Merkblätter
  → Belehrungen
  → unter Berücksichtigung der Risiken nach Art. 39 Abs. 2 EU-DSGVO
- **Unterstützung des Datenschutzbeauftragten** durch erforderliches Hilfspersonal sowie Räume, Einrichtungen, Geräte, Mittel und Fortbildungen nach Art. 38 Abs. 2 EU-DSGVO
- **Bearbeitung von Betroffenenanliegen** nach Art. 38 Abs. 4 EU-DSGVO

5.4 Datenschutzmanagement (3)

Prozesse zum Management des Mitarbeiterdatenschutzes n. **EU-DSGVO**: 2. Forts.

- **Festlegung geeigneter technischen und organisatorischer Maßnahmen** nach Art. 32 EU-DSGVO unter Berücksichtigung der Risiken nach Art. 24 Abs. 1 EU-DSGVO
- **Nachweisführung zur Einhaltung der EU-DSGVO** nach Art. 24 Abs. 1 EU-DSGVO
- **Regelmäßige Überprüfung und Aktualisierung der Schutzvorkehrungen** nach Art. 24 Abs. 1 EU-DSGVO
- **Erlass geeigneter Datenschutzrichtlinien** nach Art. 24 Abs. 2 EU-DSGVO
- **Auswahl geeigneter Auftragnehmer, deren Beratung und Überprüfung** nach Art. 28 Abs. 1 und Art. 39 Abs. 1 lit. a & b EU-DSGVO
- **Unterstützung bei den Abwägungen** nach Art. 6 Abs. 1 lit. f EU-DSGVO
- **Unterstützung bei der Meldung von Datenpannen** nach Art. 33 EU-DSGVO
- **Zusammenarbeit mit der Aufsichtsbehörde** nach Art. 39 Abs. 1 lit. d EU-DSGVO
- **Unterstützung bei der Bestimmung erforderlicher Sorgfalt** zur Vermeidung von Schadensersatz nach Art. 82 Abs. 3 EU-DSGVO

5.4 Datenschutzmanagement (4)

Prozesse zum Management des Mitarbeiterdatenschutzes nach **TMG**:

- **Unterstützung bei der Beachtung der Zweckbindung bei Einsatz von Telemedien** (§ 12 TMG)
- **Unterstützung bei der Formulierung der Datenschutzerklärung** (§ 13 Abs. 1 TMG)
- **Unterstützung bei der Festlegung der spezifischen technischen und organisatorischen Maßnahmen** nach dem Telemedienrecht (§ 13 Abs. 4 TMG)
- **Unterstützung bei der Behandlung einer Datenpanne** (§ 15a TMG)

5.4 Datenschutzmanagement (5)

Prozesse zum Management des Mitarbeiterdatenschutzes nach **BetrVG**:

- **Unterstützung bei der** Einhaltung mitbestimmungsrechtlicher Vorgaben in Verfahren zur **Leistungs- und/oder Verhaltenskontrolle** (§ 87 Abs. 1 Nr. 1 & 6 BetrVG)
  → i.d.R. im Rahmen der Datenschutz-Folgenabschätzung
- **Unterstützung bei** der Beteiligung des Betriebsrats bei **personellen Einzelmaßnahmen** (§§ 99 Abs. 1 und 102 Abs. 1 BetrVG)
- **Unterstützung bei der rechtzeitigen Information** des Betriebsrats (§§ 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. Daher keine originäre Aufgabe des Datenschutzbeauftragten.

5.5 Bestimmung des Datenschutzniveaus

Aufgabe:

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

5.5 Bestimmung des Datenschutzniveaus (1)

- Verzeichnis von Verarbeitungstätigkeiten mit Angaben aus Art. 30 EU-DSGVO vorhanden? (*kann aber i.d.R. durch Betroffenen nicht festgestellt werden*)
- Beschäftigter ausreichend über alle in diesem Verzeichnis ihn betreffenden Verfahren informiert (Gewährleistung der Transparenz)?
- 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 dem Betroffenen auf Anfrage mitgeteilt, auf welcher Rechtsgrundlage seine Daten bei einzelnen Verfahren 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?
- Genügt der Umfang der bereitgestellten Betroffenendaten im Intranet dem Grundsatz der Datenminimierung?
- Soweit ein Betriebsrat besteht: Sind in den einzelnen Betriebsvereinbarungen ausdrücklich Regelungen zum Datenschutz integriert?