Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2017:
Mitarbeiterdatenschutz (2)

4.1 Verbreitung von Bilddaten

Aufgabe:

- Ein Unternehmen möchte Bilddaten Ihrer Beschäftigten zu Zwecken der Selbstdarstellung im Internet verwenden. Wie muss das Unternehmen vorgehen, damit folgende Mitarbeitergruppen im Internet mit Portraitaufnahmen bzw. Arbeitssituationsfotos dargestellt werden dürfen?
  A) Auf der Web-Seite sollen typische Arbeitssituationen dargestellt werden. Ein professioneller Fotograf wird engagiert, interessante Bildmotive mittels entsprechender Fotografien festzuhalten.
  B) In einem sozialen Netzwerk möchte das Unternehmen Aufnahmen eines Messeauftritts im eigenen Bereich einstellen. Auf diesen Aufnahmen sind insbesondere Mitarbeiter abgebildet, wie diese auf der Messe mit Messebesuchern interagieren.
  Begründen Sie Ihre Antwort anhand EU-DSGVO, § 32 BDSG und KunstUrhG!

4.1 Verbreitung von Bilddaten (1)

- Selbstdarstellung im Internet = Offenlegung durch Verbreitung (Art. 4 Nr. 2 EU-DSGVO) für unbestimmte Empfänger (Art. 4 Nr. 9 EU-DSGVO)
- Internet = Webdienst, in dem offensichtlich Bilddaten digital gespeichert werden
- Ursprünglich angefertigte Bilddaten können aber vor Digitalisierung auch analog gewesen sein (Aufgabe hierzu nicht eindeutig) → ggf. § 22 KunstUrhG relevant
- Zweck ist die Veröffentlichung im Internet, was ausdrücklich bei einer Einwilligung als Rechtsgrundlage angegeben werden muss (gemäß einem BGH-Urteil von 2004)
- Einwilligung der Abgebildeten nötig nach Art. 6 Abs. 1 lit. a EU-DSGVO
- Die Einwilligung muss nachweisbar sein nach Art. 7 Abs. 1 EU-DSGVO
- Sind Abgebildete eindeutig erkennbar (→ rassische & ethnische Herkunft), muss sich Einwilligung ausdrücklich auf Daten nach Art. 9 Abs. 2 lit. a EU-DSGVO beziehen
- Ansonsten muss Unternehmen natürlich die üblichen Maßnahmen ergreifen (angemessener Schutz der Bilddaten nach Art. 32 EU-DSGVO und Auflistung im Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO)
- Die Durchführung einer Datenschutz-Folgenabschätzung entfällt dagegen, da keine umfangreiche Verarbeitung nach Art. 35 Abs. 3 lit. b EU-DSGVO

4.1 Verbreitung von Bilddaten (2)

Fall A) Bilddaten zur Darstellung typischer Arbeitssituationen

- Erhebung und Verwendung der Bilddaten nur mit Einwilligung der Betroffenen zulässig
- Typische Arbeitssituationen können auch durch Fotomodelle „gestellt“ werden
- Arbeitssituationen können u.U. ohne Personenbezug dargestellt werden, zu denen Personen insbesondere nur als Beiwerk im Sinne von § 23 Abs. 1 Nr. 2 KunstUrhG (d.h.: nicht wirklich erkennbar) abgebildet sind = Datenminimierung im Sinne von Art. 5 Abs. 1 lit. c EU-DSGVO
- Ergänzender Hinweis:
  Komposition des Bildmotivs räumt Fotograf Urheberrecht ein (Lichtbildwerk im Sinne von § 2 Abs. 1 Nr. 5 UrhG → Schutz nach § 72 Abs. 1 UrhG; ohne vertragliche Vereinbarung gilt § 31 Abs. 5 UrhG hinsichtlich der Nutzbarkeit)
  → Fotograf muss der Internet-Veröffentlichung ausdrücklich zustimmen und hat ein Recht daran, bei der Veröffentlichung als Urheber genannt zu werden

4.1 Verbreitung von Bilddaten (3)

Fall B) Bilddaten für Auftritt in Sozialen Netzwerken

- Messeauftritt = „ähnlicher Vorgang“ nach § 23 Abs. 1 Nr. 3 KunstUrhG
- Ggf. Betroffene nur Beiwerk zum Messegeschehen nach § 23 Abs. 1 Nr. 2 KunstUrhG
- Aber: Befugnis gilt nach § 23 Abs. 2 KunstUrhG nicht, wenn durch die Veröffentlichung ein berechtigtes Interesse des Abgebildeten verletzt wird → Abwägung nötig!
- Auf Anfertigung von Messebildern sollte ausdrücklich hingewiesen werden bzw. nur dann die Bilddaten zur Veröffentlichung im sozialen Netzwerk verwendet werden, wenn darauf keine spezifischen Personen erkennbar sind oder nur solche Personen, die ausdrücklich in die Ablichtung und Veröffentlichung eingewilligt haben
- Unternehmen ist für eigenen Auftritt im sozialen Netzwerk verantwortlich, selbst wenn das soziale Netzwerk von einer anderen Stelle betrieben wird

4.2 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.

  Hinweis: In der Aufgabenstellung müsste es korrekt „EU-DSGVO und § 32 BDSG“ statt „BDSG“ heißen!

4.2 Intranet

- Intranet = betriebsöffentliche Plattform
- Zulässigkeit hier aufgrund unterschiedlicher Rechtsgrundlagen:
  → Art. 6 Abs. 1 lit. b EU-DSGVO für zentrale Informationen über betriebliche Themen zur Erfüllung des Arbeitsvertrags (Angaben zu den Erstellern von betrieblichen Handbüchern und Wiki-Einträgen)
  → Art. 9 Abs. 2 lit. a EU-DSGVO für Bilder über Betriebsfeste (vgl. Afg. 4.1)
  → § 32 Abs. 1 BDSG für Verhaltensrichtlinien mit Newsletterfunktionalität, da Bestandteil Arbeitsvertrag, und für Accountdaten der Beschäftigten zu Intranet und Mail-Service
- 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.
- Ansonsten (wie üblich):
  ° angemessene Maßnahmen nach Art. 32 EU-DSGVO
  ° Auflistung in Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO

4.3 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 Auftragsverarbeitung erbracht wird, um weiterhin vollen Einfluss geltend machen zu können. Welche Regelungen sind zu treffen, damit diese Voraussetzung erfüllt ist? Begründen Sie Ihre Antwort!

4.3 Konzerndatenschutz (1)

- Auslagerung in zentrale Servicegesellschaft stellt Betriebsänderung im Sinne von § 111 BetrVG dar
- Vereinbarter Interessenausgleich nach § 112 Abs. 1 BetrVG schriftlich festhalten
- Konzern = Unternehmensgruppe nach Art. 4 Nr. 19 EU-DSGVO
- Verarbeitung innerhalb Unternehmensgruppe nach ErwG 48 berechtigtes Interesse nach Art. 6 Abs. 1 lit. f EU-DSGVO
- Durch Auftragsverarbeitung keine Konstruktion als Joint Control nach Art. 26 Abs. 1 EU-DSGVO
- Für Auftragsverarbeitung sind die Auflagen aus Art. 28 EU-DSGVO zu beachten, d.h. die zentral erbrachten Services müssen im Einzelnen zwischen den jeweiligen Verantwortlichen und der zentralen Servicegesellschaft (Auftragsverarbeiter) schriftlich vereinbart werden (i.d.R. via Kooperationsvertrag)
- Im vorliegenden Fall sollen neben den IT-Dienstleistungen auch HR-Dienstleistungen durch die zentrale Servicegesellschaft erbracht werden
  → Mandantentrennung einrichten
  → Aufgrund üblicher Informationspflichten gegenüber Konzernholding, sind Weitergabe und Aggregation ausdrücklich im Auftrag festzulegen
  → Zu erbringende Services sind detailliert zu beschreiben

4.3 Konzerndatenschutz (2)

- Nach Art. 28 Abs. 1 EU-DSGVO muss Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen getroffen haben
- Nach Art. 28 Abs. 3 EU-DSGVO ist im Vertrag Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des jeweiligen Verantwortlichen festzulegen
- Ausführende Beschäftigte beim Auftragsverarbeiter sind besonders auf Vertraulichkeit zu verpflichten nach Art. 28 Abs. 3 lit. b EU-DSGVO
- Aufgrund der zu erbringenden IT-Dienstleistungen ist zudem der Zugriff auf weitere personenbezogene Daten des jeweiligen Verantwortlichen nicht ausschließbar

4.4 Kontrolle Webnutzung

Aufgabe:

- Ein Unternehmen möchte die Web-Nutzung ihrer Mitarbeiter im eingesetzten Content-Management-System mitprotokollieren. Dabei soll aufgezeichnet werden, von welchem Rechner (IP-Adresse) welche Web-Seite aufgerufen wurde und wie viele Klicks unter dieser URL getätigt wurden. Die aufgerufenen Web-Seiten sollen nach Möglichkeit kategorisiert und dabei ausgewertet werden, welche Kategorien von den Mitarbeitern am stärksten frequentiert werden. Im Unternehmen ist die private Nutzung des Internets in geringem Umfang während der Arbeitszeit gestattet. Ist die vollständige Aufzeichnung Ihrer Ansicht nach zulässig? Begründen Sie Ihre Antwort!

4.4 Kontrolle Webnutzung (1)

- IP-Adresse (= Online-Kennung) ist für Verantwortlichen personenbezogen, da die IT-Abteilung jederzeit die zugehörigen Rechner zuordnen kann, d.h. welcher Account (= Mitarbeiter) sich dahinter verbirgt (s.a. ErwG 30)
  → Protokollierung der IP-Adressen personenbezogen
- Unternehmen möchte durch Protokollierung Kenntnis über den Ressourceneinsatz bekommen = berechtigtes Interesse nach Art. 6 Abs. 1 lit. f EU-DSGVO
  → Abwägung erforderlich!
- Aufzeichnung des Klickverhaltens = Verhaltenskontrolle → Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 lit. a EU-DSGVO nötig!
- Zweck der Aufzeichnung ist nur die Kategorisierung und Nutzungsgewichtung der aufgerufenen Web-Seiten → Personenbezug aus IP-Adresse entbehrlich
- In Content Management System darf daher nur die aufgerufene Webseite mitgeloggt werden, nicht aber die IP-Adresse des aufrufenden Rechners! (wg. Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c EU-DSGVO)
- Aufgrund der gestatteten Privatnutzung fungiert der Arbeitgeber als TK-Access-Provider, wobei die Nutzungsdaten nicht unter das Fernmeldegeheimnis fallen (gemäß dem Urteil LAG LAG Berlin-Brandenburg v. 2011)

4.4 Kontrolle Webnutzung (2)

- Gegen die Aufzeichnung der Nutzungsdaten bestehen offensichtlich keine überwiegenden Betroffeneninteressen, wenn die IP-Adressen der aufrufenden Rechner nicht mitprotokolliert werden
- Laut Aufgabenstellung ist aber eine vollständige Aufzeichnung geplant
  → Die vollständige Aufzeichnung ist aber zur Zweckerfüllung nicht erforderlich und damit auch nicht verhältnismäßig!
  → **Geplante Aufzeichnung unzulässig**!

4.5 Einsicht in E-Mail-Postfach

Aufgabe:

- In einem Unternehmen ist die Privatnutzung der dienstlich zur Verfügung gestellten Mail-Adressen ausdrücklich untersagt. Das Unternehmen hat einen Betriebsrat. Unter welchen Umständen darf bei Abwesenheit der Mail-Postfach-Inhaber in deren elektronisches Postfach Einblick genommen werden? Begründen Sie Ihre Antwort! Beachten Sie dabei, dass der Mail-Dienst ein Telemediendienst ist.

4.5 Einsicht in E-Mail-Postfach (1)

- Der Abschnitt zum Datenschutz aus dem TMG gilt nicht für Telemedien, wenn der E-Mail-Dienst ausschließlich zu beruflichen und dienstlichen Zwecken erfolgt (nach § 11 Abs. 1 Nr. 1 TMG)
- Da die Privatnutzung der elektronischen Kommunikationsmedien bei dem Unternehmen ausdrücklich verboten ist, gilt folglich diese Prämisse
- Einsicht in E-Mail-Postfach erfolgt auf der Grundlage von Art. 6 Abs. 1 lit. f EU-DSGVO → Abwägung erforderlich!
- Hinweise:
  - ° Fernmeldegeheimnis aus § 88 TKG gilt selbst bei gestatteter Privatnutzung nicht im Beschäftigungsverhältnis (Urteil LAG Berlin-Brandenburg v. 2011) → zudem ist der Beschäftigte kein Dritter im Sinne von § 3 Nr. 10 TKG
  - ° E-Mails, die im Postfach des Empfängers eingegangen sind, unterliegen dem informationellen Selbstbestimmungsrecht (Urteil BVerfG v. 2006)
  - ° Selbst bei gestatteter privater Nutzung darf dies nur in einem angemessenen Umfang erfolgen (Urteil BAG v. 2005)
  - ° dienstlich bedingte Nutzung in privaten Angelegenheiten (Terminvereinbarung mit Ärzten & Behörden, Mitteilung über Arbeitsende) ist keine Privatnutzung

4.5 Einsicht in E-Mail-Postfach (2)

- Bei Einblick in E-Mail-Postfach zu beachten:
  - ° bei aktuell beschäftigten Mitarbeitern ohne leitende Funktion darf der Betriebsrat der Einsichtnahme beiwohnen aufgrund des Mitbestimmungsrechts (§ 80 Abs. 1 Nr. 1 BetrVG)
  - ° bei ausgeschiedenen Mitarbeitern und leitenden Angestellten ist der Betriebsrat nicht zuständig (wegen § 5 Abs. 1 & 3 BetrVG)
  - ° bei jeder Einsichtnahme ist der Zweck der Einsichtnahme vorab festzulegen aufgrund Grundsatz der Zweckbindung aus Art. 5 Abs. 1 lit. b EU-DSGVO
  - ° Mails ausschließlich für dienstliche Korrespondenz bestimmt, dennoch können sich in eingegangen Mails private Mails befinden → Einsicht eingeschränkt
  - ° bei Mitarbeitern mit besonderer Schutzfunktion (z.B. Betriebsrat, Schwerbehindertenvertretung, Datenschutzbeauftragter, Betriebsarzt, Beauftragter für Arbeitssicherheit, Gleichbehandlungsbeauftragter, Personalleitung, Geschäftsführung) ist ein zweites Paar Augen mit gleichem Schutzniveau nötig (im Zweifel der Datenschutzbeauftragte)
  - ° der Mitarbeiter ist nach seiner Rückkehr über die erfolgte Einsichtnahme zu unterrichten