Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2014:
Mitarbeiterdatenschutz (1)

2.1 Verfahrensverzeichnis

Aufgabe:

- Erstellen Sie anhand der Auflistung aus § 4e BDSG das vom Datenschutzbeauftragten nach § 4g Abs. 2 BDSG zu veröffentlichende "Verfahrensverzeichnis" für nachfolgend benannte Verfahren zum Mitarbeiterdatenschutz:
  - Bewerbungsverfahren
  - Personalaktenführung
  - Lohn- und Gehaltsabrechnung.

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (1)

- **Öffentliches Verfahrensverzeichnis** = Auflistung der Punkte 1 – 8 aus § 4e BDSG (nach § 4g Abs. 2 BDSG)
- Verwaltung von Mitarbeiterdaten = eigene Geschäftszwecke
- Bewerbungsverfahren im Einklang mit § 32 Abs. 1 BDSG = Verfahren zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses
- Personalaktenführung im Einklang mit § 32 Abs. 1 BDSG = Verfahren zur Durchführung eines Beschäftigungsverhältnisses (nach dessen Begründung)
- Lohn- und Gehaltsabrechnung im Einklang mit § 32 Abs. 1 BDSG = Verfahren zur Durchführung eines Beschäftigungsverhältnisses (nach dessen Begründung)

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (2)

Betroffenengruppen & Datenkategorien:

- Bewerbungsverfahren
  → Betroffene: Bewerber
  → Datenkategorien: Namensdaten, Bilddaten, sonstige Identifikationsdaten, Kontaktdaten, Bewerbungsdaten (Angaben zu Bildungsabschlüssen, Berufserfahrung, Sprachkenntnissen, Motivation für Bewerbung, etc.)

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (3)

Betroffenengruppen & Datenkategorien:

- Personalaktenführung
  → Betroffene: Beschäftigte und ehemalige Beschäftigte
  → Datenkategorien: Namensdaten, Bilddaten, sonstige Identifikationsdaten, Kontaktdaten, Bewerbungsdaten, Qualifikationsdaten (über berufliche Fortbildung, erhaltene Einweisungen, etc.), Vertragsdaten (zum Anstellungsvertrag, inkl. Personalverwaltungsdaten wie Personalnummer, Stellenbezeichnung, Zuordnung zur Organisationseinheit, Steuerdaten, Krankenversicherungsdaten, Daten über Bankkonto, Schwerbehinderungsgrad etc.), Leistungsdaten (sofern Leistungsprämien oder dgl.), Verhaltensdaten (für den Fall von Abmahnungen)

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (4)

Betroffenengruppen & Datenkategorien:

- Lohn- und Gehaltsabrechnung
  → Betroffene: Beschäftigte
  → Datenkategorien: 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.)

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (5)

1. Name oder Firma der verantwortlichen Stelle:
   XY GmbH & Co. KG
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen:
   Geschäftsführer: Peter Müller
   Personalleiter: Josef Schmidt
   EDV-Leiterin: Andrea Schulze
3. Anschrift der verantwortlichen Stelle:
   XY GmbH & Co. KG
   Musterstr. 1
   12345 Musterstadt

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (6)

4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung:
   A) Bewerbungsverfahren
   B) Personalaktenführung
   C) Lohn- und Gehaltsabrechnung
5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien:
   Betroffene A): Bewerber
   Betroffene B): ehemalige Beschäftigte
   Betroffene B) und C): Beschäftigte
   Datenkategorien A): Namensdaten, Bilddaten, sonstige Identifikationsdaten, Kontaktdaten, Bewerbungsdaten
   Datenkategorien B): Namensdaten, Bilddaten, sonstige Identifikationsdaten, Kontaktdaten, Bewerbungsdaten, Qualifikationsdaten, Vertragsdaten, Leistungsdaten, Verhaltensdaten

2.1 Verfahrensverzeichnis für Mitarbeiterdatenverwaltung (7)

5. Datenkategorien C): Namensdaten, sonstige Identifikations-daten, Vertragsdaten, Leistungsdaten
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:
   A): interne Stellen (ausschreibende Stelle, Betriebsrat) zur Aufgabenerfüllung
   B): interne Stellen (Finanzbuchhaltung) zur Aufgabenerfüllung
   C): öffentliche Stellen aufgrund gesetzlicher Vorgaben
7. Regelfristen für die Löschung der Daten:
   A): 6 Monate (Anschreiben ohne Anhänge),
   B): 10 Jahre nach Beschäftigungsende,
   C): 10 Jahre (Buchungsdaten)
8. eine geplante Datenübermittlung in Drittstaaten:
   A), B) und C): entfällt

2.2 Mitbestimmung

Aufgabe:

- Ein Unternehmen, das über einen Betriebsrat verfügt, möchte neben den drei grundlegenden Verfahren aus Aufgabe 2.1 eine Arbeitszeit-überwachung einführen (Arbeitszeiten, Krankheitsausfallzeiten, Weiter-bildungszeiten, unproduktive Zeiten). Welche Anforderungen aus BDSG und BetrVG hat das Unternehmen dabei zu beachten?

2.2 Mitbestimmung (1)

- Arbeitszeitüberwachung = Verhaltenskontrolle
  → Vorabkontrolle nötig nach § 4d Abs. 5 BDSG, die durch den Datenschutzbeauftragten nach § 4d Abs. 6 BDSG durchzuführen ist
  → Mitbestimmung nach § 87 Abs. 1 Nr. 1 BetrVG, da Arbeitszeit-Verhalten der Arbeitnehmer im Betrieb Gegenstand ist, und ggf. nach § 87 Abs. 1 Nr. 6 BetrVG, wenn das Arbeitszeit-Verhalten mittels technischer Einrichtung überwacht wird, die zur Überwachung auch bestimmt ist (hierzu keine nähere Angabe in der Aufgabe)
  → Nach § 80 Abs. 2 BetrVG ist der Betriebsrat vom Arbeitgeber rechtzeitig & umfassend über geplante Einführung zu unterrichten (bzw. nach § 90 Nr. 2 BetrVG im Fall der technischen Einrichtung)

2.2 Mitbestimmung (2)

- Arbeitszeitüberwachung = Verfahren zur Durchführung des Beschäftigungsverhältnisses (Einhaltung arbeitsvertraglich vereinbarter Arbeitszeiten)
  → Rechtsgrundlage: § 32 Abs. 1 BDSG
  → Beteiligungsrechte des Betriebsrats bleiben nach § 32 Abs. 3 BDSG unberührt
  → trotz gesetzlicher Regelung besteht Mitbestimmung nach § 87 Abs. 1 BetrVG fort
  → Betriebsrat kann insbesondere den Datenschutzbeauftragten als Sachverständigen nach § 80 Abs. 3 BetrVG hinzuziehen
- Üblicherweise wird zu diesem Verfahren eine Betriebsvereinbarung zwischen Betriebsrat und Arbeitgeber vereinbart

2.2 Mitbestimmung (3)

- Weitere Anforderungen:
  - ° Nur erforderliche Arbeitszeitdaten erheben und verwenden
  - ° Arbeitszeitdaten unterliegen grundsätzlich der Zweckbindung, Zweckänderungen würden einer Abwägung nach § 28 Abs. 2 Nr. 1 BDSG i.V.m. § 28 Abs. 1 Nr. 2 BDSG bedürfen
  - ° Verpflichtung der mit der Arbeitszeitüberwachung beschäftigten Personen auf das Datengeheimnis nach § 5 BDSG (gilt damit auch für die Betriebsrats-Mitglieder, da das Datengeheimnis ergänzend zur Geheimhaltungsverpflichtung aus § 79 BetrVG hinzutritt!)
  - ° Ergreifung ausreichender technischer & organisatorischer Maßnahmen nach § 9 BDSG
  - ° Aufbewahrung der Arbeitszeiten gemäß gesetzlicher Fristen (6 Jahre nach § 147 Abs. 1 Nr. 5 AO)

2.2 Mitbestimmung (4)

- Weitere Anforderungen (Ergänzung außerhalb der Übung):
  - ° Aufgrund der spezifischen Aufbewahrungsfrist aus § 16 Abs. 2 ArbZG sind Überstunden ab 2 Jahren gesperrt nach § 35 Abs. 3 Nr. 1 BDSG (wg. der AO-Vorgabe)
  - ° Aufgrund der spezifischen Aufbewahrungsfrist aus § 3 Abs. 1 Nr. 2 EntgFG sind Daten über Arbeitsunfähigkeiten nach 1 Jahr gesperrt nach § 35 Abs. 3 Nr. 1 BDSG (wg. der AO-Vorgabe)
  - ° Daten über Arbeitsunfähigkeiten = Gesundheitsdaten (Daten über zeitweise nicht vorhandener Gesundheit)
    - → nötig zur Rechtsausübung des Arbeitgebers im Sinne von § 28 Abs. 6 Nr. 3 BDSG (Ausgleichszahlungen durch Krankenkassen)

2.3 Datenschutzrisiko gemäß Vorabkontrolle

Aufgabe:

- Das Unternehmen aus 2.2 möchte am Betriebsrat vorbei ein System zur Personalentwicklung einführen. Die Personalabteilung möchte damit folgende Wünsche umsetzen:
  ° Anhand der im Bewerbungsverfahren eingereichten Zeugnisse soll ermittelt werden, welcher Fortbildungsbedarf anhand der zugeordneten Stellenbeschreibung für erfolgreiche Bewerber besteht.
  ° Die Arbeitszeitdaten aus der Arbeitszeitüberwachung sollen mit den Produktivitätsdaten, die bereits im Rahmen der Betriebsdatenerfassung erhoben wurden, im Sinne von Leistungsdaten korreliert werden, um feststellen zu können, welche Mitarbeiter besonders produktiv sind.
  ° Ermittelte Leistungsdaten sollen in den einzelnen Produktionsbereichen als Top 10 ausgehängt werden, um so Nichtplatzierte zu höheren Leistungen zu motivieren.
  ° Anhand der Daten aus den jährlichen Mitarbeitergesprächen soll ermittelt werden, welche Mitarbeiter für spezialisierte Aufgaben, insbesondere zur Teamleitung, geeignet sind und welche Fortbildungsmaßnahmen dafür notwendig sind.
  ° Zu jeder Fortbildung haben die Mitarbeiter Bewertungen anzugeben, wie nützlich und wie teuer genossene Fortbildungen waren.
  Geben Sie an, welche potenziellen Datenschutzrisiken Sie im Rahmen einer Vorabkontrolle (gem. § 4d Abs. 5 BDSG) sehen, schätzen Sie die Eintrittsstufe dieser Datenschutzrisiken ab und ermitteln Sie den Handlungsbedarf gemäß nachstehender 3x3-Risk-Map. Sofern Handlungsbedarf besteht, geben Sie eine passende, zu ergreifende Schutzmaßnahme an.

2.3 Datenschutzrisiko gemäß Vorabkontrolle (1)

A) Ermittlung potenzieller Datenschutzrisiken:

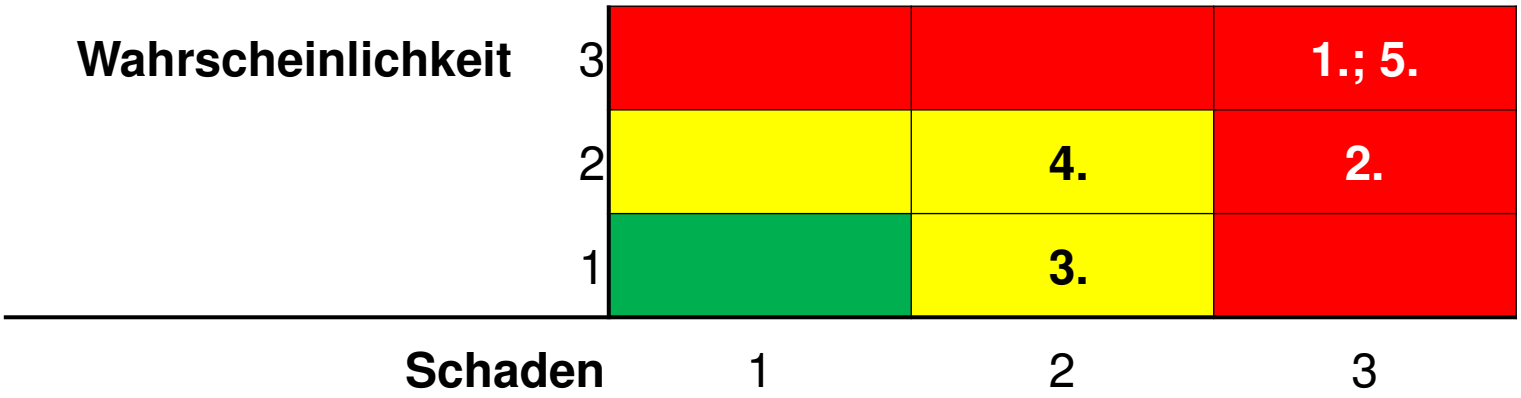
- Personalentwicklung am Betriebsrat vorbei
  1. Verletzung Mitbestimmungsrecht → strafbare Behinderung der Tätigkeit des Betriebsrats (§ 119 Abs. 1 Nr. 2 BetrVG)
  2. Infolge der Nichtbeachtung des Mitbestimmungsrechts unzulässiges Verfahren → ordnungswidriges Erheben & Verarbeiten der Personalentwicklungsdaten (§ 43 Abs. 2 Nr. 1 BDSG)
- Auswertung Zeugnisdaten (Fähigkeitsdaten) für Fortbildungsbedarf
  3. Zweckänderung von Fähigkeitsdaten ohne Abwägung → formaler Verstoß
- Abgleich mit Leistungsdaten aus Betriebsdatenerfassung
  4. Zweckänderung von Leistungsdaten ohne Abwägung → formaler Verstoß
- Aushang der Leistungsdaten (= Veröffentlichung einer sog. „Rennliste“)
  5. Unbefugte Übermittlung von Leistungsdaten → ordnungswidriges Verarbeiten der Leistungsdaten (§ 43 Abs. 2 Nr. 1 BDSG)
- Auswertung Mitarbeitergespräche für Personalentwicklung → ordnungsgemäß!
- Bewertung erhaltener Fortbildungen → ggf. potenzieller Neidfaktor (außerhalb DS!)

2.3 Datenschutzrisiko gemäß Vorabkontrolle (2)

B) Abschätzung der Eintrittsstufe:

1. Verletzung Mitbestimmungsrecht: Eintritt sicher, da auch Betriebsratsmitglieder von Verfahren betroffen sind
2. Infolge der Nichtbeachtung des Mitbestimmungsrechts unzulässiges Verfahren: Eintritt wahrscheinlich, da zugleich mit Mitbestimmungsverstoß verbunden
3. Zweckänderung von Fähigkeitsdaten ohne Abwägung: Eintritt möglich, aber unwahrscheinlich (zulässige Datenverwendung, wenn mit Abwägung durchgeführt)
4. Zweckänderung von Leistungsdaten ohne Abwägung: Eintritt wahrscheinlich, da Leistungskontrolle der Mitbestimmung unterliegt
5. Unbefugte Übermittlung von Leistungsdaten: Eintritt sicher, da innerbetriebliche Veröffentlichung von allen Betroffenen ausdrücklich zur Kenntnis genommen werden soll

2.3 Datenschutzrisiko gemäß Vorabkontrolle (3)



Rot = Aktivität nötig; **Gelb** = Aktivität prüfen; **Grün** = Akzeptabel

Wahrscheinlichkeit: **Eintritt einer Verletzung des informationellen Selbstbestimmungsrechts**	**Schaden:** **Grad der Verletzung des informationellen Selbstbestimmungsrechts**
1 = möglich	1 = niedrig (ohne unmittelbare Wirkung)
2 = wahrscheinlich	2 = mittel (formaler Verstoß)
3 = sicher	3 = hoch (Bußgeld/Datenpanne)

2.3 Datenschutzrisiko gemäß Vorabkontrolle (4)

C) Handlungsempfehlung:

1. Verletzung Mitbestimmungsrecht
   → Betriebsrat einbeziehen!
2. Infolge der Nichtbeachtung des Mitbestimmungsrechts unzulässiges Verfahren
   → durch Maßnahme zu 1. erledigt
3. Zweckänderung von Fähigkeitsdaten ohne Abwägung
   → Abwägung vornehmen
4. Zweckänderung von Leistungsdaten ohne Abwägung
   → Abwägung vornehmen & Betriebsrat einbeziehen
5. Unbefugte Übermittlung von Leistungsdaten
   → unterlassen, da unverhältnismäßiger Eingriff!

2.4 Bewerbungsverfahren & soziale Netzwerke

Aufgabe:

- Ein Unternehmen möchte über seine Bewerber Angaben aus sozialen Netzwerken auswerten, um daraus Kenntnisse zu gewinnen, ob die Bewerber, die im sozialen Netzwerk mit einem eigenen Profil vertreten sind, anhand von deren allgemein sichtbaren Angaben als geeignete Bewerber anzusehen sind. Ist diese Auswertung der veröffentlichten Daten im Bewerbungsverfahren zulässig? Begründen Sie Ihre Antwort!

2.4 Bewerbungsverfahren & soziale Netzwerke (1)

- Soziales Netzwerk = privatrechtliche Plattform, mit der die jeweiligen Nutzer ein rechtsgeschäftliches Schuldverhältnis eingegangen sind
  → Soziales Netzwerk weist i.d.R. Nutzungsbedingungen auf
  → Soziales Netzwerk geht mit personenbezogenen Nutzungsdaten um und beschreibt daher datenschutzrechtliche Aspekte in einer eigenen Datenschutzerklärung
- Nur allgemein sichtbare Angaben der Nutzer werden ausgewertet
  → Öffentlich zugängliche Daten dürfen nach § 28 Abs. 1 Nr. 3 BDSG für eigene Geschäftszwecke verwendet werden!
  → Ausschluss an Verwendung nur gegeben, wenn Betroffeneninteresse offensichtlich dagegen spricht
  → Gründe gegen Verwendung: Offenbarung der Daten innerhalb eines bestimmten Kontextes (soziales Netzwerk), aber: veröffentlichte Daten allgemein zugänglich, d.h. ohne Zugriffsschutz abrufbar

2.4 Bewerbungsverfahren & soziale Netzwerke (2)

- Nur allgemein sichtbare Angaben der Nutzer werden ausgewertet (Forts.)
  → Daten zulässig veröffentlicht, wenn diese vom Betroffenen selbst eingestellt wurden
  → keine Daten auswerten, die von anderen Nutzern über die Betroffenen eingestellt wurden! → **führt sonst zur Unzulässigkeit!**
  → Daten dürfen nur dann ausgewertet werden, wenn man sich zum Abruf der Daten nicht am sozialen Netzwerk anmelden muss (sonst potenzieller Verstoß gegen Nutzungsbedingungen und ggf. überwiegender Ausschlussgrund für Betroffene) → **werden Daten erst nach entsprechender Anmeldung am sozialen Netzwerk ausgewertet, wäre Datenverwendung unzulässig!**
  → nur Daten auswerten, die über Suchmaschinen oder öffentlich verfügbare Suchfunktionen des sozialen Netzwerks abrufbar sind

2.4 Bewerbungsverfahren & soziale Netzwerke (3)

- Ausgewertet werden sollen Daten von und über Bewerbende
  → § 32 Abs. 1 BDSG einschlägig: Daten zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses
  → § 32 Abs. 1 BDSG ersetzt zwar § 28 Abs. 1 Nr. 1 BDSG (gemäß der Gesetzesbegründung), nicht aber § 28 Abs. 1 Nr. 3 BDSG
  → unter Beachtung der Vorgaben auf den vorangegangenen Seiten ist das geplante Vorgehen datenschutzrechtlich **zulässig**! (und in der Praxis auch üblich)

2.5 Digitalisierung von Personalakten

Aufgabe:

- Ein Unternehmen möchte seine bisher auf Papier geführten Personalakten digitalisieren. Welche technischen und organisatorischen Maßnahmen sollte das Unternehmen dabei ergreifen, damit die digitalen Personalakten einem angemessenen Schutz unterliegen? Berücksichtigen Sie dabei, dass sich in den Personalakten besondere Arten personenbezogener Daten, Kontodaten und Persönlichkeitsprofildaten befinden.

2.5 Digitalisierung von Personalakten (1)

- Nach Aufgabe 2.1 beinhalten Personalakten folgende Datenkategorien: Namensdaten, Bilddaten, sonstige Identifikationsdaten, Kontaktdaten, Bewerbungsdaten, Qualifikationsdaten (über berufliche Fortbildung, erhaltene Einweisungen, etc.), Vertragsdaten (zum Anstellungsvertrag, inkl. Personalverwaltungsdaten wie Personalnummer, Stellenbezeichnung, Zuordnung zur Organisationseinheit, Steuerdaten, Krankenversicherungsdaten, Daten über Bankkonto, Schwerbehinderungsgrad etc.), Leistungsdaten (sofern Leistungsprämien oder dgl.), Verhaltensdaten (für den Fall von Abmahnungen)
  → **hoher Schutzbedarf** der zu speichernden Daten!

2.5 Digitalisierung von Personalakten (2)

Maßnahmen zur innerbetrieblichen Organisation:

- Verpflichtung der Zugriffsbefugten auf das Datengeheimnis
- Bestellung eines Datenschutzbeauftragten
- Schulung der Zugriffsbefugten über Datenschutz

Maßnahmen zur Zutrittskontrolle:

- Personalbereich & Serverraum jeweils getrennte Sicherheits-zonen
- Personalbüros in Abwesenheit der HR-Mitarbeiter verschlossen
- Serverraum nur mit Chipkarte betretbar unter Aufzeichnung des Zutritts
- Vergabe nur erforderlicher Zutrittsbefugnisse

2.5 Digitalisierung von Personalakten (3)

Maßnahmen zur Zugangskontrolle:

- Vergabe von Zugangsbefugnissen nur für Befugte
- Authentifikation mittels personalisierter Benutzerkennung und ausreichend langem & komplexen Passwort
- Einsatz einer Bildschirmsperre bei 15 minütiger Inaktivität
- Regelmäßige Prüfung der eingeräumten Zugangsbefugnisse
- Unverzüglicher Zugangsrechteentzug bei vorliegender Nicht-erforderlichkeit

2.5 Digitalisierung von Personalakten (4)

Maßnahmen zur Zugriffskontrolle:

- Einsatz eines detaillierten Berechtigungskonzepts mit klarer Beschränkung vergebener Zugriffsrechte
- Unterscheidung von Zugriffsbefugnissen nach Unterlagenarten, z.B. besonderer Zugriffsschutz auf Schwerbehindertenunterlagen
- Regelmäßige Prüfung der eingeräumten Zugriffsrechte
- Unverzüglicher Zugriffsrechteentzug bei vorliegender Nichterforderlichkeit
- Temporäre Zugriffsgewährung (für Betroffenen vollständig und für Vorgesetzte nur anteilig) unter Anwesenheit von HR-Mitarbeitern

2.5 Digitalisierung von Personalakten (5)

Maßnahmen zur Weitergabekontrolle:

- Server mit Firewall und Netzwerksegregation gesichert
- Export für andere Anwendungen (z.B. Lohn- und Gehaltsdaten-übeweisung) über dedizierte Schnittstellen
- Remote-Zugriff auf digitalisierte Personalakten nur nach Freigabe durch zuständigen HR-Mitarbeiter mit Interventionsrecht des HR-Mitarbeiters (darf Verbindung trennen)
- Zugriffsrechte von Betroffene und Vorgesetzte umfassen keine Exportrechte, sondern nur Anzeigerechte (und Druckrechte)
- Fehldrucke sind unter Einhaltung der DIN 66399 Stufe P-4 zu vernichten

2.5 Digitalisierung von Personalakten (6)

Maßnahmen zur Eingabekontrolle:

- Protokollierung der Eingabe der Digitalisierungsdaten
- Protokollierung erfolgter Einsichtnahmen in die Personalakte
- Protokollierung von Systemzugriffen

Maßnahmen zur Auftragskontrolle:

- Etwaig vergebene Auftragstätigkeiten nur unter Beachtung von § 11 BDSG

2.5 Digitalisierung von Personalakten (7)

Maßnahmen zur Verfügbarkeitskontrolle:

- Papierne Personalunterlagen, die nach § 2 Abs. 1 NachwG (und anderen spezialrechtlichen Auflagen) schriftlich vorzuhalten sind, werden ergänzend auf Papier vorgehalten
- Datenbank mit Personalaktendaten redundant auslegen
- Personalaktendaten sind täglich auf Backups zu sichern
- Backupdaten werden in einem anderen Brandabschnitt gelagert
- Regelmäßige Prüfung der Wirksamkeit der Datensicherung
- Server mit ausreichend dimensionierter USV betrieben

2.5 Digitalisierung von Personalakten (8)

Maßnahmen zur Trennungskontrolle:

- Ein Datenexport ist nur nach vorheriger Vorabkontrolle zulässig
- Personalaktendaten werden in unterschiedliche Segmente aufgeteilt (Stammdaten, Bewerbungsdaten, Exportdaten, Gesundheitsdaten, …)