

Muster

Beispiel für ein internes Verzeichnisse, das als Arbeitshilfe für den bDSB und die Belegschaftsvertretung dient.

Personalverwaltungs- und Abrechnungssystem

Rechtliche Grundlagen: Die Inhalte des Verzeichnisses ergeben sich aus § 4e und § 4g Abs. 2 BDSG. Zusätzlich sind noch betriebsbezogene Inhalte aufzunehmen, die der bDSB für seine Aufgabenerfüllung benötigt. Das folgende ausgefüllte Verzeichnisse erhebt nicht den Anspruch auf Vollständigkeit (z.B. bei Daten oder Datenkategorien) oder letztendliche Konsistenz (Personalabrechnungs- und -verwaltungssystem einschließlich Arbeitszeiterfassung). Das „Muster“ setzt sich aus Beratungsbeispielen, aus Vorlagen der Aufsichtsbehörden und Eckpunkten aus Beispielen von Prof. Peter Gola und Dr. Thomas B. Petri zusammen.¹

Angaben zur verantwortlichen Stelle (§ 4e Satz 1 Nr. 1-3 BDSG)

1. Name oder Firma der verantwortlichen Stelle

XYZ-Klinik in XYZ

2.1 Leiter der verantwortlichen Stelle und der Datenverarbeitung; Datenschutzbeauftragte(r)

- Geschäftsführerin Frau Dr. XYZ;
- Leiter IT-Abteilung Herr XYZ;
- Datenschutzbeauftragter des Klinikums Herr XYZ

2.2 Organisationsbereich(e), Software-Komponenten

Bereich XX, Standort XXX

- Zentrale Personalverwaltung, nähere Auskunft erteilt: Frau XYZ, Personalleiterin; Herr XXX, EDV-Leiter

Software-Komponenten

- PA Personalmanagement
- PT Zeitwirtschaft
- PY Personalabrechnung

3. Anschrift der verantwortlichen Stelle

- Straße:
- Postleitzahl:
- Ort:



Angaben zu den Datenverarbeitungsverfahren (§ 4e Satz 1 Nr. 4-8 BDSG) mit internen Ergänzungen

4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung, Rechtsgrundlagen

Personalabrechnung und -verwaltung	Rechtsgrundlagen
<ul style="list-style-type: none"> • Erfüllung sozialversicherungsrechtlicher Verpflichtungen • Erfüllung gesetzlicher Meldepflichten • Entgeltabrechnung • Arbeitszeiterfassung • Terminverwaltung • Reisekostenabrechnung • Datenaustausch mit Geldinstituten • Statistische Auswertungen • Zeiterfassung/Dienstplan 	<ul style="list-style-type: none"> • § 32 BDSG „Beschäftigungsverhältnis“ • Arbeitsvertrag • Tarifvertrag • Betriebsvereinbarung (fehlt bislang, ist erforderlich) • Einkommenssteuergesetz • Lohnsteuergesetz • Datenerfassungs- und -übermittlungsverordnung - DEÜV • § 829 Abs. 2 Satz 1 ZPO (Gehaltspfändungen) • § 16 Abs. 2 ArbZG und § 7d Abs. 1 Satz 1 SGB IV - Arbeitszeitkonten Wertguthabenvereinbarung

5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien, Herkunft

Personengruppen	Daten/Datenkategorie/Herkunft
<ul style="list-style-type: none"> • Beschäftigte der Klinik XYZ • Bewerber • Ehemalige Beschäftigte • Aushilfen • Führungskräfte 	<ul style="list-style-type: none"> • Name • Daten zur Person • Personalnummer • Staatsangehörigkeit • Behinderung • Familie/Bezugsperson • Adressdaten (Anschrift) • Geburtsdatum • Andere/frühere Arbeitgeber

	<ul style="list-style-type: none"> • Qualifikationen • Ein- und Austritt • Lohn- und Gehaltsdaten/Abrechnungsdaten • Renten- und Sozialversicherungsdaten • Bankverbindung • Vermögensbildung • Vertragsbestandteile • Pfändungen • Zeugnisse • Abmahnungen • Bewerbungsunterlagen • Zeiterfassungsdaten (Abwesenheiten, Anwesenheiten, Dienstpläne, Zusatzurlaub) • Gehaltsentwicklung • Betriebliche Altersversorgung <p>Herkunft:</p> <ul style="list-style-type: none"> •  Personalfragebogen, Arbeitsvertrag •  Direkterhebung •  Bescheinigung Arbeitnehmer •  Self Service Mitarbeiter
--	---

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

<ul style="list-style-type: none"> • Personalabteilung, Lohnbuchhaltung: Abrechnung der lohnrelevanten Daten • Betriebsrat: Leserecht Überwachung Zeitdaten, Stammdaten • Personalplanung: Dienstplanung, Zeitwirtschaft • Controlling/Revision: nur anonymisierte Daten • Vorgesetzte des betroffenen Beschäftigten: Mitarbeitergespräch, Arbeitszeitkonto • Kreditinstitute: Gehaltsüberweisung • Gläubiger: Lohn- und Gehaltspfändungen • Finanzamt: Lohn- und Gehaltsdaten • Sozialversicherungsträger: Krankenversicherungen, Ärzteversorgungskassen, Rentenversicherungsträger

- Externer Auftragsdatenverarbeiter: Datenträgerentsorgung, Fernwartung

7. Regelfristen für die Löschung der Daten

Daten/Datenkategorien	Regelfristen/Rechtsgrundlage
Lohnberechnungsunterlagen Lohnkonten, Gehaltslisten Quittungsbelege über den Arbeitslohn Reisekostenabrechnung	6 Jahre, Belege zum Lohnkonto: 10 Jahre § 147 Abs. 1 Nr. 4, 5 i.V.m. Abs. 3 AO (Abgabenordnung); § 41 Abs. 1 Satz 9 EStG § 257 Abs. 1 Nr.4, 5 i.V.m. § 238 Abs. 1 HGB
Abmahnung	2 bis 2,5 Jahre, Rechtsprechung Arbeitsgerichte
Bewerbungsdaten	Unverzüglich nach Entscheidung über Nichtbesetzung zwei Monate Diskriminierungsbeweislast- Frist § 22 AGG Ansonsten: bei Auflösung Arbeitsverhältnis
Arbeitszeitrachweise nach § 16 Abs. 2 ArbZG Arbeitszeitrachweise Arbeitszeitrachweise	2 Jahre: nach § 16 Abs. 2 ArbZG 2 Jahre: § 50 JArbSchG 6 Jahre, § 147 Abs. 1 Nr. 5, Abs. 3 AO i.V.m. § 3b EStG

8. Geplante Datenübermittlung in Drittstaaten

geplant: ja nein

Wenn ja: im Zusammenhang mit Auslandseinsätzen

Zweck	Daten/Datenkategorie	Länder/Länderkategorie
Auslandseinsatz	Daten zur Person	USA

9. Allgemeine Beschreibung der geplanten Maßnahmen nach § 9 und Anlage zu § 9 BDSG

Organisationskontrolle	Einhaltung Datengeheimnis, Verpflichtung der Mitarbeiter
	Datenschutzrichtlinie, aktualisiert und auf Beschäftigtendatenschutz bezogen
	Festlegung der Aufbewahrungsfristen für die

	einzelnen Daten und Dateien
	Erstellung einer aussagekräftigen Verfahrensdokumentation
Zutrittskontrolle	Zutritt Personalabteilung: nur Mitarbeiter der Abteilung Abschließen der Räume mit Sicherheitsschlössern Protokollierung der ein- und ausgehenden Personen Zutritt Server: EDV-Mitarbeiter
Zugangskontrolle	Passwortschutz Zurücksetzen der Bildschirmmaske Firewall Viren-Checker und Spam-Filter History-Funktionen von Programmen, z.B. SAP
Zugriffskontrolle	Reduzierung der Zahl der Super-User und Administratoren
	Berechtigungskonzept mit Rollen und unterschiedlichen Berechtigungsstufen
	Regelungen für den Verhinderungsfall/Stellvertreter
	Zuordnung Benutzerprofil/Rechner/Person
	Automatisierte Protokollierung und Auswertung der Protokolldatei
	Datenträgervernichtung durch Auftragnehmer: sorgfältige Auswahl, schriftlicher Vertrag nach § 11 BDSG Protokollierung der Fernwartungszugriffe
Weitergabekontrolle	Personalabteilung: Verschlüsselung der Daten beim E-Mail-Versand
Eingabekontrolle	Protokollierung (Log-Dateien)
Auftragskontrolle	Vertrag mit Firma XXX-Franz nach § 11 BDSG laufende Audits, Kontrollen vereinbart
Verfügbarkeitskontrolle	Risiko- und Schwachstellenanalyse liegt vor Schulung Mitarbeiter hinsichtlich Sicherheitsanforderungen Angriff von außen: Firewall
Trennungsgebot	Personalabrechnungsdaten auf eigenem Server oder Mandanten

10. Zugriffsberechtigungen nach § 9 und Anlage Nr. 3 zu § 9 Nr. 3 BDSG (Berechtigungsmatrix)

Personengruppen	Zugriff Daten, Datenkategorien, Berechtigungen	Aktivitäten
Administratoren	Getrennt : Benutzerverwaltung, Berechtigungsverwaltung und -vergabe	Einrichten
Personalsachbearbeiter	Zuständig für Mitarbeiter A-H	Ändern
Personalleiter	Für alle Mitarbeiter	Löschen
Betroffener (Mitarbeiter)	Kann alle seine Daten einsehen	Einsichtnahme
Vorgesetzter	Nur Mitarbeiter seines Teams, nur temporärer Einblick in Personaleinsatzplan	
Revisoren	Nur anonyme Daten	
Betriebsrat	Ständiger Zugriff	Lesen

¹ Für den öffentlich-rechtlichen Bereich siehe das Muster nach § 8 DSG NRW mit vorangehenden Erläuterungen, in: Lübking/Zilkens, Datenschutz in der Kommunalverwaltung. Recht. Technik. Organisation, 3. Auflage, 2011, 151 - 158