
Shiftbase-Vorlage

Umgang mit Mitarbeiterdaten & Datenschutz | Grundsätze + Checkliste



Erstellt von





Über diese Vorlage

Diese Vorlage richtet sich an Inhaber, Führungskräfte, HR-Verantwortliche und alle Personen, die mit Mitarbeiterdaten arbeiten – z. B. Dienstpläne, Zeiterfassung, Abwesenheiten, Gehaltsdaten, Leistungsbeurteilungen oder Personalakten.

Sie ist praxisnah formuliert und hilft dir dabei, Datenschutz alltagstauglich, DSGVO-konform und einheitlich umzusetzen.

Wozu dient es?

- Klare und praktikable Regeln für den täglichen Umgang mit Mitarbeiterdaten
- Reduktion von „versehentlichen Datenpannen“ (falscher Link, falscher Empfänger, unübersichtliche Tabellen)
- Einheitliche Prozesse für Zugriff, Speicherung, Aufbewahrung und den Umgang mit Datenschutzvorfällen
-

So nutzt du die Vorlage (Einrichtung in ca. 20 Minuten)

1. Fülle die Platzhalter aus (Datenschutzbeauftragte, zugelassene Tools, Speicherorte, Aufbewahrungsgrundlagen).
2. Lege ein zentrales System für Dienstplanung, Zeiterfassung und Abwesenheiten fest ("Single Source of Truth").
3. Prüfe die Zugriffsrechte:
 - Wer braucht welche Daten wirklich?
 - Wer sollte keinen Zugriff haben?
 - Wie wird der Zugriff beim Offboarding entzogen?

4. Integriere die Regeln in Onboarding und Führungskräftebildungen (5 Minuten reichen).

⚠ Wichtiger Hinweis:

Diese Vorlage orientiert sich an der DSGVO und dem deutschen Datenschutzrecht, ersetzt jedoch keine Rechtsberatung. Tarifverträge, Betriebsvereinbarungen und branchenspezifische Vorgaben können zusätzliche Anforderungen enthalten.

Richtlinie: Datenschutz & Mitarbeiterdaten

Zweck	Du schützt die personenbezogenen Daten deiner Mitarbeitenden und stellst sicher, dass diese rechtmäßig, sicher und respektvoll verarbeitet werden.
Geltungsbereich	Gilt für alle Mitarbeiterdaten, die erhoben, gespeichert, genutzt, weitergegeben oder gelöscht werden – einschließlich: Personalakten, Dienst- und Zeitdaten, Abwesenheits- und Urlaubsaufzeichnungen, Lohn- und Vergütungsdaten, Leistungs- und Disziplinarakten, Bewerbungsunterlagen, Schulungs- und Qualifikationsnachweise.

Was zählt zu Mitarbeiterdaten? (Beispiele)

- Identitäts- und Kontaktdaten
- Arbeitszeiten und geleistete Stunden
- Abwesenheits- und Urlaubszeiten
- Lohn-, Gehalts- und Vergütungsdaten
- Leistungs-, Feedback- und Disziplinarakten
- Bewerbungsunterlagen (Lebensläufe, Interviewnotizen, Referenzen)
- Zertifikate und Schulungsnachweise

!! Grundregeln (verbindlich)

Erstellt von

- **Datensparsamkeit:** Erfasse nur Daten, die du für einen klaren Zweck wirklich brauchst.
- **Zugriff beschränken:** Nur Personen mit berechtigtem Bedarf erhalten Zugriff.
- **Zugelassene Systeme nutzen:** Keine Speicherung in privaten E-Mail-Postfächern, Messenger-Diensten oder losen Dateien.
- **Daten aktuell halten:** Korrigiere Fehler und aktualisiere veraltete Informationen zeitnah.
- **Nicht unbegrenzt speichern:** Halte Aufbewahrungsfristen ein und lösche Daten, sobald sie nicht mehr benötigt werden.
- **Vorfälle sofort melden:** Jeder Verdacht auf Datenmissbrauch oder -verlust muss umgehend gemeldet werden.

Wo dürfen Mitarbeiterdaten gespeichert werden?

Zentrales HR-/Zeiterfassungssystem:

Datentyp:	Tool:
Dienstplanung	
Zeiterfassung:	
Abwesenheit:	
Lohnabrechnung:	

Weitere zulässige Speicherorte

- Personalunterlagen: [Tool/System + Ordner/Pfad]
- Bewerberdaten: [ATS / Tool + Pfad]
- Unterzeichnete Dokumente (Verträge etc.): [Tool/System]

✗ Nicht erlaubt

Erstellt von

- Private Laufwerke, private E-Mail-Adressen, öffentlich zugängliche Ordner oder Links mit „Jeder mit dem Link“.

Zugriffsregeln (rollenbasiert & einfach)

- **HR-Zugriff:** [Rollen]
- **Führungskräfte:** Zugriff nur auf Daten der direkt unterstellten Mitarbeitenden (Planung, Genehmigungen, Leistung).
- **Lohnabrechnung:** Zugriff nur auf zwingend erforderliche Daten.
- **Admin-Zugriff:** Nur namentlich benannte Personen, regelmäßige Überprüfung (mind. quartalsweise).

Zugriffsprüfung

- Überprüfung mindestens vierteljährlich oder bei organisatorischen Änderungen
- Sofortiger Entzug bei Rollenwechsel oder Austritt

Regeln für das Teilen von Daten

Bevor du Mitarbeiterdaten weitergibst, frage dich:

- Wird diese Information wirklich benötigt?
- Reicht eine Zusammenfassung statt der kompletten Datei?
- Ist der Zugriff beschränkt?
- Ist der/die Empfänger:in korrekt?

✗ Niemals teilen

- Gesundheitsdaten, Disziplinarakten oder Ausweisdokumente in Gruppenchats oder großen E-Mail-Verteilern.

Aufbewahrung von Mitarbeiterdaten (Grundlinie)

Du speicherst Mitarbeiterdaten nur so lange, wie sie erforderlich sind für:

- Personalverwaltung
- gesetzliche Pflichten
- legitime betriebliche Zwecke

Beispielhafte Aufbewahrungsfristen (anzupassen):

Erstellt von

- Recruiting-Unterlagen: [X Monate/Jahre]
- Lohnabrechnung: [X Jahre]
- Disziplinarakten: [X Monate/Jahre]
- Zeit- & Anwesenheitsdaten: [X Jahre]

Anfragen von Mitarbeitenden

Mitarbeitende haben das Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten im Rahmen der gesetzlichen Vorgaben.

➡ Leite entsprechende Anfragen weiter an: [Name & E-Mail Datenschutzbeauftragter]

Datenschutzvorfälle – was ist sofort zu tun?

Ein Vorfall kann z. B. sein: falscher E-Mail-Empfänger, verlorenes Gerät, offener Tabellenlink, kompromittiertes Passwort.

Vorgehen

1. **Schaden begrenzen:** Zugriff entziehen, Links deaktivieren, Passwörter ändern.
2. **Datenschutzbeauftragte informieren:** [Name/Kontakt]
3. **Vorfall dokumentieren:** Was ist passiert? Welche Daten? Wer ist betroffen? Wann?
4. **Nachbereitung:** Ursache beheben, Prozesse/Schulungen anpassen, Abschluss dokumentieren.

+ Add-ons & Arbeitshilfen

Datenschutz-Schnellcheck (vor dem Teilen)

- ☐ Ist es die minimal nötige Information?
- ☐ Ist der Zugriff eingeschränkt?
- ☐ Habe ich die Empfänger geprüft?

Erstellt von

☐ Wäre eine Weiterleitung vertretbar?

Übersicht Mitarbeiterdaten (Tabelle – kopieren & ausfüllen)

Datentyp	System	Verant- wortlich	Wer hat Zugriff?	Aufbewahr- ung	Notizen
Terminplan ung					
Zeiterfassung					
Abwesenheit/ Urlaub					
Lohnabrechnung					
Verträge					
Werbung					
Leistung/Disziplin					

Verhaltensregeln für Führungskräfte

✓ Do	✗ Don't
Nutze zugelassene Systeme	Keine privaten Tools für Mitarbeiterdaten
Halte Notizen sachlich und arbeitsbezogen	Keine sensiblen Infos in Gruppenchats

Erstellt von

Beschränke Links und Zugriffe	Keine offenen Tabellen oder ungeschützten Links
Entziehe Zugriffe bei Rollenwechsel oder Austritt	Keine wertenden oder subjektiven Begriffe in Notizen

Vorlage: Datenschutzvorfall (intern)

Thema:	Datenschutzvorfall
Datum/Uhrzeit der Entdeckung:	
Meldende Person:	
Beschreibung des Vorfalls:	
Betroffene Daten:	
Betroffene Personen:	
Sofortmaßnahmen:	
Nächste Schritte + Verantwortliche:	
Status: Offen / In Bearbeitung / Abgeschlossen	

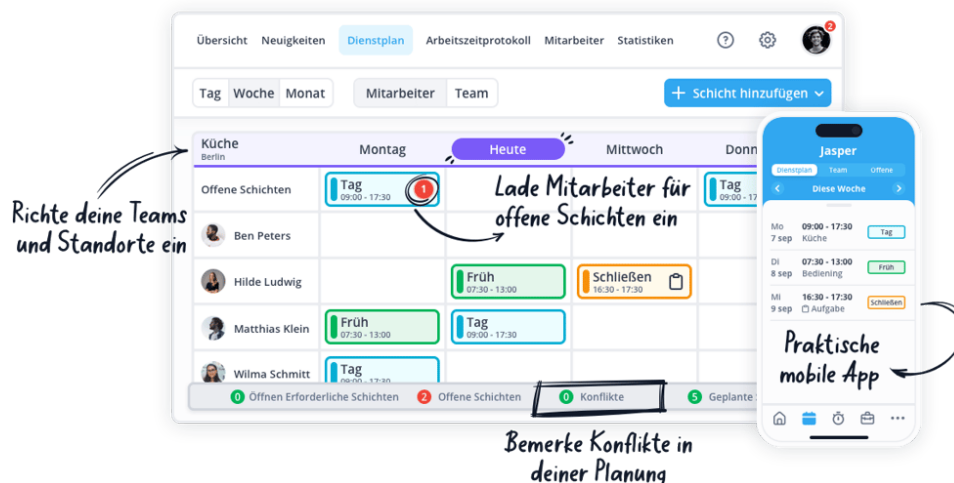
Probiere Shiftbase 14 Tage kostenlos aus.



JETZT SHIFTBASE KOSTENLOS & UNVERBINDLICH FÜR 14 TAGE TESTEN

Verwalte alle Mitarbeiterdaten zentral an einem Ort und behalte den Überblick über dein gesamtes Unternehmen. Mit aussagekräftigen Analysen, individuellen Reports und übersichtlichen Dashboards erhältst du Einblicke in deine Unternehmensleistung – jederzeit und in Echtzeit.

Shiftbase hilft dir dabei, HR-Prozesse zu vereinfachen und dein Unternehmen effizienter zu steuern.



JETZT KOSTENLOS TESTEN

Erstellt von

