NAMARU

# SOP-Bibliothek — Leseprobe

4 von 40 SOPs als kostenfreie Vorschau. Das vollständige Paket (12 Kategorien, PDF + editierbare DOCX-Templates) erhalten Sie über Namaru.

**12 Kategorien · 40 SOPs**
Version 1.0 · Stand Juni 2026
Namaru — Wissens-Archiv + async Consulting für deutsche KMU

KATEGORIE VERWALTUNG · SOP 01.1

# Urlaubsantrag stellen und genehmigen

| | |
|---|---|
| Zweck | Urlaub wird planbar, fair und rechtssicher genehmigt — ohne Engpässe im Team und ohne verlorene Anträge. |
| Geltungsbereich | Alle Mitarbeitenden mit Urlaubsanspruch nach BUrlG. |
| Version / Stand | v1.0 · Juni 2026 · Prozessverantwortlich: ‹Name, Rolle› |

## ROLLEN UND ZUSTÄNDIGKEITEN

| Rolle | Aufgabe in diesem Prozess |
|---|---|
| Mitarbeiter/in | Antrag rechtzeitig stellen |
| Führungskraft | Teamabdeckung prüfen, genehmigen oder ablehnen |
| HR / Verwaltung | Resturlaub pflegen, Antrag archivieren |

## ABLAUF

1. Urlaubsantrag mit Zeitraum und Vertretung einreichen (mind. 2 Wochen vorher) — Mitarbeiter/in

▼

2. Resturlaub und Teamkalender prüfen — Führungskraft

▼

3. **Teamabdeckung im Zeitraum gesichert?** — Führungskraft
   **Ja →** weiter mit Schritt 4 (genehmigen) · **Nein →** weiter mit Schritt 5 (Alternativtermin)

▼

4. Antrag genehmigen, Vertretung bestätigen, HR informieren — Führungskraft

▼

5. Alternativtermin mit Mitarbeiter/in abstimmen, dann erneut ab Schritt 2 — Führungskraft

▼

6. Urlaub im HR-System erfassen, Resturlaub aktualisieren — HR / Verwaltung

## CHECKLISTE

- ☐ Antrag mindestens 2 Wochen vor Antritt gestellt
- ☐ Vertretung benannt und informiert
- ☐ Resturlaub geprüft, kein negativer Saldo
- ☐ Genehmigung schriftlich dokumentiert
- ☐ Abwesenheit im Teamkalender sichtbar

## DOKUMENTATION (WER / WANN / WIE / WOMIT)

| Was wird dokumentiert | Wer | Wann | Ablage / Werkzeug |
|---|---|---|---|
| Urlaubsantrag mit Genehmigung | HR / Verwaltung | bei Genehmigung | HR-System / Personalakte |

> **Hinweis:** Gesetzlicher Mindesturlaub (§ 3 BUrlG): 24 Werktage bei 6-Tage-Woche. Ablehnung nur aus dringenden betrieblichen Gründen (§ 7 BUrlG).

## FREIGABE

| Rolle | Name | Datum | Unterschrift |
|---|---|---|---|
| Erstellt | | | |
| Geprüft | | | |
| Freigegeben (Leitung) | | | |

KATEGORIE IT & DATENSCHUTZ · SOP 04.1

# IT-Sicherheitsvorfall melden (Incident-Reporting)

| | |
|---|---|
| **Zweck** | Sicherheitsvorfälle werden sofort gemeldet und strukturiert behandelt — Schaden wird begrenzt statt verschleppt. |
| **Geltungsbereich** | Alle Mitarbeitenden; alle IT-Sicherheitsvorfälle und Verdachtsfälle (Phishing, Malware, unbefugter Zugriff). |
| **Version / Stand** | v1.0 · Juni 2026 · Prozessverantwortlich: ‹Name, Rolle› |

## ROLLEN UND ZUSTÄNDIGKEITEN

| Rolle | Aufgabe in diesem Prozess |
|---|---|
| Mitarbeiter/in | Vorfall sofort melden, nichts vertuschen |
| IT-Verantwortliche/r | Bewertung, Eindämmung, Behebung |
| Geschäftsführung | Eskalation, externe Meldungen |

## ABLAUF

1. Vorfall sofort an IT melden (Telefon/definierter Kanal) — Gerät nicht ausschalten, nicht weiterarbeiten — Mitarbeiter/in

▼

2. Vorfall bewerten: betroffene Systeme, Daten, Ausbreitungsrisiko — IT-Verantwortliche/r

▼

3. Eindämmen: Gerät vom Netz trennen, Zugänge sperren, Passwörter zurücksetzen — IT-Verantwortliche/r

▼

4. **Personenbezogene Daten betroffen (Datenschutzverletzung)?** — IT-Verantwortliche/r
   **Ja →** SOP Datenleck-Response starten (72-h-Frist!) · **Nein →** weiter mit Schritt 5

▼

5. Vorfall beheben, Systeme aus sauberem Backup wiederherstellen — IT-Verantwortliche/r

▼

6. Vorfallsbericht erstellen: Hergang, Maßnahmen, Lessons Learned — IT-Verantwortliche/r

## CHECKLISTE

- ☐ Meldung ohne Verzögerung (auch bei Eigenfehler — keine Sanktion fürs Melden)
- ☐ Betroffene Systeme identifiziert und isoliert
- ☐ Datenschutz-Relevanz geprüft
- ☐ Wiederherstellung aus verifiziertem Backup
- ☐ Bericht mit Lessons Learned erstellt

## DOKUMENTATION (WER / WANN / WIE / WOMIT)

| Was wird dokumentiert | Wer | Wann | Ablage / Werkzeug |
|---|---|---|---|
| Vorfallsbericht | IT-Verantwortliche/r | innerhalb 3 Werktagen nach Abschluss | IT-Dokumentation / ISMS |

> **Hinweis:** Meldekultur: Wer einen Fehler meldet, wird nicht bestraft. Verschleppte Vorfälle sind teurer als gemeldete.

## FREIGABE

| Rolle | Name | Datum | Unterschrift |
|---|---|---|---|
| Erstellt | | | |
| Geprüft | | | |
| Freigegeben (Leitung) | | | |

KATEGORIE RECHNUNGSWESEN · SOP 06.1

# Eingangsrechnung prüfen und freigeben

| | |
|---|---|
| Zweck | Nur sachlich und rechnerisch geprüfte Rechnungen werden bezahlt — Doppelzahlungen und Fake-Rechnungen werden verhindert. |
| Geltungsbereich | Alle Eingangsrechnungen. |
| Version / Stand | v1.0 · Juni 2026 · Prozessverantwortlich: ‹Name, Rolle› |

## ROLLEN UND ZUSTÄNDIGKEITEN

| Rolle | Aufgabe in diesem Prozess |
|---|---|
| Buchhaltung | Formale Prüfung, Erfassung, Zahlung |
| Besteller/in / Fachabteilung | Sachliche Prüfung |
| Geschäftsführung | Freigabe ab Schwellenwert |

## ABLAUF

1. Rechnung erfassen, Pflichtangaben prüfen (§ 14 UStG: USt-ID, Rechnungsnummer, Leistungsdatum) — Buchhaltung

▼

2. Sachliche Prüfung: Leistung erbracht, Preis wie vereinbart, Bestellung vorhanden? — Besteller/in

▼

3. **Betrag über Freigabegrenze (z. B. 1.000 €)?** — Buchhaltung
   **Ja →** Zweitfreigabe durch GF einholen (4-Augen-Prinzip) · **Nein →** weiter mit Schritt 4

▼

4. Rechnung zur Zahlung freigeben, Skontofrist vermerken — Buchhaltung

▼

5. Zahlung im nächsten Zahllauf ausführen (Skonto nutzen) — Buchhaltung

▼

6. Beleg GoBD-konform archivieren — Buchhaltung

## CHECKLISTE

- ☐ Pflichtangaben nach § 14 UStG vollständig
- ☐ Sachliche Prüfung durch Besteller dokumentiert
- ☐ 4-Augen-Prinzip ab Schwellenwert
- ☐ Skontofristen genutzt
- ☐ Keine Zahlung auf erstmalig genannte/geänderte Bankverbindung ohne Rückruf-Verifikation

## DOKUMENTATION (WER / WANN / WIE / WOMIT)

| Was wird dokumentiert | Wer | Wann | Ablage / Werkzeug |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Geprüfte Rechnung mit Freigabevermerk | Buchhaltung | je Rechnung | Buchhaltungssystem / DMS, 8 Jahre |

> **Hinweis:** Betrugsprävention: Bankverbindungs-Änderungen eines Lieferanten immer über bekannte Telefonnummer verifizieren (CEO-Fraud / Fake-Rechnungen).

## FREIGABE

| Rolle | Name | Datum | Unterschrift |
|---|---|---|---|
| Erstellt | | | |
| Geprüft | | | |
| Freigegeben (Leitung) | | | |

KATEGORIE KRISENMANAGEMENT & KOMMUNIKATION · SOP 12.1

# Datenleck-Response (Datenschutzverletzung)

| | |
|---|---|
| **Zweck** | Datenschutzverletzungen werden eingedämmt, fristgerecht gemeldet (72 h!) und sauber aufgearbeitet. |
| **Geltungsbereich** | Alle Verletzungen des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO). |
| **Version / Stand** | v1.0 · Juni 2026 · Prozessverantwortlich: ‹Name, Rolle› |

## ROLLEN UND ZUSTÄNDIGKEITEN

| Rolle | Aufgabe in diesem Prozess |
|---|---|
| **Entdeckende Person** | Sofort intern melden |
| **Datenschutz-Koordinator/in / DSB** | Bewertung, Meldung, Dokumentation |
| **IT-Verantwortliche/r** | Technische Eindämmung |
| **Geschäftsführung** | Entscheidung und Verantwortung |

## ABLAUF

1. Verdacht sofort an Datenschutz-Koordinator und IT melden — Uhr läuft ab Kenntnis! — Entdeckende Person

▼

2. Eindämmen: Zugriff stoppen, Systeme isolieren, Beweise sichern — IT-Verantwortliche/r

▼

3. Bewerten: Welche Daten, wie viele Betroffene, welches Risiko für Betroffene? — Datenschutz-Koordinator/in

▼

4. **Risiko für Rechte und Freiheiten der Betroffenen?** — Datenschutz-Koordinator/in

   **Ja →** Meldung an Aufsichtsbehörde binnen 72 h ab Kenntnis (Art. 33 DSGVO) · **Nein →** Verletzung intern dokumentieren (Begründung, warum keine Meldung), weiter mit Schritt 6

▼

5. **Hohes Risiko für Betroffene (z. B. Konto-, Gesundheitsdaten)?** — Datenschutz-Koordinator/in

   **Ja →** Betroffene unverzüglich benachrichtigen (Art. 34 DSGVO) · **Nein →** weiter mit Schritt 6

▼

6. Ursache beheben, Maßnahmen ableiten, vollständige Dokumentation erstellen — Datenschutz-Koordinator/in

## CHECKLISTE

- ☐ Meldekette bekannt, 72-h-Frist eingehalten
- ☐ Eindämmung vor Aufklärung (erst stoppen, dann analysieren)
- ☐ Risikobewertung dokumentiert (auch bei Nicht-Meldung)
- ☐ Betroffenen-Benachrichtigung bei hohem Risiko
- ☐ Maßnahmen gegen Wiederholung umgesetzt

## DOKUMENTATION (WER / WANN / WIE / WOMIT)

| Was wird dokumentiert | Wer | Wann | Ablage / Werkzeug |
|---|---|---|---|
| Verletzungsdokumentation (Art. 33 Abs. 5 DSGVO) | Datenschutz-Koordinator/in | je Vorfall, vollständig | Datenschutz-Ordner |
| Meldung + Behördenkorrespondenz | Datenschutz-Koordinator/in | binnen 72 h | Datenschutz-Ordner |

> **Hinweis:** Die 72-h-Frist läuft ab Kenntnis der Verletzung — nicht ab Abschluss der Analyse. Lieber fristgerecht mit Teilinformationen melden und nachreichen.

## FREIGABE

| Rolle | Name | Datum | Unterschrift |
|---|---|---|---|
| Erstellt | | | |
| Geprüft | | | |
| Freigegeben (Leitung) | | | |