01_Governance & Compliance

- Rechtliche Grundlagen
  - DSGVO – Überblick
  - GoBD – Verfahrensdokumentation (Vorlage)
  - Aufbewahrungsfristen (HGB/AO)
  - BSI IT-Grundschutz – Basis-Absicherung (WiBA)
- Rollen & Verantwortlichkeiten
  - Rollenmatrix & Stellvertretungen
- Richtlinien
  - Policy – Informationssicherheit
  - Policy – Datenklassifizierung & Schutzbedarf
  - Policy – Passwort & MFA
  - Policy – Zugriff & Berechtigungen (IAM)
  - Policy – Logging & Aufbewahrung

Rechtliche Grundlagen

DSGVO – Überblick

DSGVO – Überblick

Geltungsbereich: Gesamtes Unternehmen inkl. mobiler Arbeit
Rollen: Verantwortlicher (GF), Datenschutzkoordination, IT-Leitung, Fachbereiche
Schwerpunkte: Verzeichnis von Verarbeitungstätigkeiten (Art. 30), TOMs (Art. 32), AV-Verträge (Art. 28), Betroffenenrechte, Löschkonzept

Verantwortlichkeiten

- **Verantwortlicher:** {{Firma, GF}}
- **Datenschutz-Kontakt:** {{E-Mail}}
- **Datenschutzbeauftragter (falls Pflicht/benannt):** {{intern/extern, Name, Kontakt}}

Nachweise in dieser Doku

- VVT (Prozesse), TOMs, AV-Vertragsspiegel, DSFA (falls erforderlich-Für Spiegelblank nicht erforderlich)
- Was ist ein AV-Vertragsspiegel?

Der AV-Vertragsspiegel ist kein rechtliches Musterdokument, sondern ein Organisationsinstrument: Eine zentrale, gepflegte Liste aller Dienstleister mit AV-Vertrag inkl. der wichtigsten Metadaten. Typisch ist das eine Tabelle (Excel, GLPI, DMS, BookStack, Confluence, …) mit Einträgen wie: Dienstleister/ System (z. B. „Microsoft 365“, „GLPI Cloud“, „Rechenzentrum X“) Rolle: Auftragsverarbeiter / gemeinsam Verantwortlicher / sonstiger Empfänger Verarbeitungszweck (z. B. E-Mail & Kollaboration, Ticketsystem, Backup, Hosting) Kategorien personenbezogener Daten (Mitarbeiterdaten, Kundendaten, IP-Adressen, Logdaten …) Kategorien Betroffener (Mitarbeiter, Kunden, Bewerber, Lieferanten …) Rechtsgrundlage (z. B. Art. 6 Abs. 1 lit. b, c, f DSGVO) AV-Vertrag vorhanden? (Ja/Nein, Datum des Abschlusses) Ablageort des AV-Vertrags (Pfad im DMS/SharePoint/Ordner) Auftragsverarbeiter-Sitz / Datenverarbeitung (EU/EWR, Drittland, Standardvertragsklauseln etc.) technische und organisatorische Maßnahmen (TOM) geprüft? (Ja/Nein, Datum) Datenschutz-Freigabe (z. B. „Freigegeben durch DSB am 15.08.2025“) Anmerkungen (z. B. „Enthält Gesundheitsdaten“, „Joint Controllership mit XY“, …)

- Meldejournal Datenschutzvorfälle, Betroffenenrechte-Prozess, Löschkonzept

> *Hinweis:* Dieses Dokument ist eine Arbeitsvorlage und ersetzt keine Rechtsberatung.

GoBD – Verfahrensdokumentation (Vorlage)

GoBD-Verfahrensdokumentation

Version: 1.0 | **Owner:** Finanz/IT | **Letztes Review:** *TT.MM.JJJJ*
Geltungsbereich: Alle steuerrelevanten IT-gestützten Prozesse/Systeme

1 Zweck & Zielbild

Sicherstellung von Nachvollziehbarkeit, Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung & Unveränderbarkeit.

2 Organisation & Verantwortlichkeiten

- Rollen (Finanz, IT, Fachbereiche), Vertretungen, Schulungen
- Berechtigungskonzept (rollenbasiert), Vier-Augen-Prinzip bei Änderungen

3 Steuerrelevante Prozesse

- Eingangs-/Ausgangsrechnungen, Löhne/Gehälter, Kasse, Anlagenbuchhaltung, Reisekosten
- Belegfluss (Scan, Erfassung, Prüfung, Freigabe, Archivierung)

4 IT-Systeme, Schnittstellen & Datenflüsse

- Systemliste (ERP, FiBu, DMS, E-Mail/Archiv, Exportformate)
- Schnittstellen inkl. Prüfsummen/Protokolle

5 Belegwesen & Aufbewahrung

- Erfassung, Indexierung/Metadaten, Versionierung
- Unveränderbarkeit (technisch/organisatorisch), Aufbewahrungsfristen

6 Datensicherung & Notfall

- Backup-Strategie (RPO/RTO), Testprotokolle, Wiederanlauf

7 Änderungskontrolle (Change-Management)

- Planung, Test, Freigabe, Dokumentation, Rückfallstrategie

8 Interne Kontrollen & Self-Checks

- Turnus, Prüflisten, Abweichungsbehandlung, Maßnahmenjournal

Anhänge: Prozessdiagramme, Belegfluss, Export-/Schnittstellenbeschreibungen, Protokolle

#todo FIBU

Aufbewahrungsfristen (HGB/AO)

Aufbewahrungsfristen (Überblick)

Dokumentart	Frist	Start Fristlauf	Ablageort/System
Bücher, Inventare, Jahresabschlüsse	10 Jahre	Jahresende	{{DMS/Archiv}}
Buchungsbelege	10 Jahre	Jahresende	{{DMS/Archiv}}
Geschäfts-/Handelsbriefe (empfangen/versandt)	6 Jahre	Jahresende	{{DMS/Archiv}}

Technische Umsetzung: Sperr- und Löschfristen in DMS/Archiv, Nachweis über Löschprotokolle.
Verweis: Löschkonzept (DIN 66398) & GoBD-Verfahrensdoku.

BSI IT-Grundschutz – Basis-Absicherung (WiBA)

BSI IT-Grundschutz – Basis-Absicherung (WiBA)

Scope: Nicht-KRITIS, KMU-geeigneter Einstieg.
Vorgehen (Kurz): Schutzbedarf → Basis-Absicherung → Maßnahmenpriorisierung → Umsetzung → Wirksamkeitsprüfung → kontinuierliche Verbesserung.

Dieses Kapitel verlinkt auf: Policy IS, TOMs, Notfallmanagement, Patch/SIEM, Awareness.

Rollen & Verantwortlichkeiten

Rollenmatrix & Stellvertretungen

Rollenmatrix & Stellvertretungen

Rolle	Kernaufgaben	Stellvertretung	Kompetenzen	Genehmigungen
IT-Leitung	IS-Policy, Roadmap, Freigaben	{{Name}}	{{…}}	{{…}}
Datenschutz-Koordination	VVT/TOMs/AV, Meldungen	{{Name}}	{{…}}	{{…}}
Admin AD/M365	Betrieb, Changes, Notfall	{{Name}}	{{…}}	{{…}}

Richtlinien

Richtlinien

Policy – Informationssicherheit

Informationssicherheits-Policy

Version: 1.0 | **Owner:** IT-Leitung | **Geltungsbereich:** Unternehmensweit

Ziel

Schutz von Vertraulichkeit, Integrität, Verfügbarkeit (VIA) auf Basis eines risikoorientierten Ansatzes.

Grundsätze

- Minimalprinzip (Least Privilege), MFA standard, Netzwerksegmentierung
- Härtung & Patchen, Protokollierung & Auswertung, Backup/BCM
- Sensibilisierung & Schulung, Lieferantensteuerung

Mindestanforderungen

- Passwort- & MFA-Vorgaben, Endgeräte-Verschlüsselung, Admin-Protokollierung
- Patchfenster & Schwachstellenbehebung
- Notfallmanagement inkl. Übungen

Verweise

- TOMs (Art. 32), Notfallhandbuch (BSI 200-4), GoBD-Verfahrensdoku, Patch/Vuln-Prozess

Richtlinien

Policy – Datenklassifizierung & Schutzbedarf

Policy – Datenklassifizierung & Schutzbedarf

Klassen: Öffentlich · Intern · Vertraulich · Streng vertraulich
Kennzeichnung: Dokument-/System-Tags, Ordnerstruktur, Watermark (falls möglich)

Beispiele:

- *Vertraulich:* Mitarbeiter-, Kunden-, Finanzdaten
- *Intern:* Prozessdokumente, Betriebsanweisungen

Schutzbedarf: Auswirkung auf Vertraulichkeit, Integrität, Verfügbarkeit → Maßnahmen ableiten.

Richtlinien

Policy – Passwort & MFA

Policy – Passwort & MFA

- **MFA** verpflichtend für Admins, Remote/VPN, Cloud
- **Passwörter:** ausreichend lang, Manager empfohlen, keine Wiederverwendung
- **Servicekonten:** Kennworttresor, Rotation, keine interaktive Anmeldung
- **Reset-Prozess:** Identitätsprüfung, Protokollierung

Richtlinien

Policy – Zugriff & Berechtigungen (IAM)

Policy – Zugriff & Berechtigungen (IAM)

- Rollenbasiert (RBAC), **Need-to-know**
- Joiner-Mover-Leaver (JML) Prozess verbindlich
- Adminrechte nur temporär (Just-in-Time), Vier-Augen-Prinzip
- Regelmäßige Rezertifizierung (z. B. halbjährlich), Nachweise dokumentieren

Richtlinien

Policy – Logging & Aufbewahrung

Policy – Logging & Aufbewahrung

Pflichtquellen: AD, Firewalls, VPN, kritische Server/Anwendungen
Inhalte: An-/Abmeldungen, Admin-Aktionen, Policy-Änderungen, Fehler/Eskalationen
Aufbewahrung: gem. Schutzbedarf/DSGVO/GoBD
Auswertung: Dashboards/Alerts (LibreNMS, Wazuh/OpenSearch/Graylog), Monatsreport als Nachweis