Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

- BilanZen – Externe Finanzbuchhaltung & Backoffice für KMU und Steuerkanzleien

Inhaberin: Patrycja Pourian, Gosepfad 43, 21037 Hamburg
Stand: 01.12.2025 – Geltungsbereich: B2B

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen („TOMs"), die die Auftragsverarbeiterin zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus gemäß Art. 32 DSGVO getroffen hat. Sie gelten für alle Verarbeitungen personenbezogener Daten im Rahmen der zwischen den Parteien geschlossenen Auftragsverarbeitungsvereinbarung.

Hinweis: Die Auftragsverarbeiterin wird als Einzelunternehmen geführt. Die nachfolgend beschriebenen Maßnahmen sind auf eine schlanke, aber wirksame Organisation und eine überwiegend digitale, remote-basierte Arbeitsweise ausgerichtet.

1. Organisation und Verantwortlichkeiten

- Die Auftragsverarbeiterin (BilanZen) ist für die datenschutzkonforme Ausgestaltung der im Rahmen der Auftragsverarbeitung eingesetzten Prozesse und Systeme verantwortlich.
- Verantwortlichkeiten für Datenschutz und Informationssicherheit sind intern eindeutig der Inhaberin zugeordnet; bei Bedarf werden spezialisierte Dienstleister (z. B. IT-Administration, Datenschutzberatung) hinzugezogen.
- Personen, die unterstützend tätig werden (z. B. freie Mitarbeit), werden vor Aufnahme der Tätigkeit auf Vertraulichkeit verpflichtet und erhalten eine Einweisung in die maßgeblichen Datenschutz- und Sicherheitsanforderungen.
- Es wird ein Verzeichnis von Verarbeitungstätigkeiten geführt, das die relevanten Prozesse (z. B. Finanzbuchhaltung, Reporting, Kundenverwaltung, Kundenportal) dokumentiert.

2. Systemlandschaft und Hosting

- Die produktiven Systeme (Webseite, Kundenbereich, Admin-Backend und Datenbank) werden auf einem virtuellen Linux-Server (Ubuntu) bei der Hetzner Online GmbH, Deutschland, betrieben.
- Die Anwendung ist in Docker-Containern strukturiert (u. a. Web-Applikation auf Basis von Next.js, PostgreSQL-Datenbank, Reverse Proxy mit Caddy).
- Der Server-Standort befindet sich in einem Rechenzentrum in Deutschland; Hetzner stellt eigene TOMs zur Verfügung und wird als Unterauftragsverarbeiter in die AVV aufgenommen.
- Zugriffe auf die öffentlich erreichbare Webseite und den Kundenbereich erfolgen ausschließlich über HTTPS (TLS); das TLS-Zertifikat wird automatisiert verwaltet.

3. Zutrittskontrolle (physischer Zugang)

Ziel: Unbefugten Personen wird der physische Zutritt zu Räumen und Geräten, in denen personenbezogene Daten verarbeitet werden, verwehrt.

Maßnahmen u. a.:

- Arbeitsräume sind nicht öffentlich zugänglich; Türen sind außerhalb der Arbeitszeiten verschlossen.
- Mobile Endgeräte (Notebook) werden bei Abwesenheit sicher verwahrt bzw. mitgenommen.
- Papierunterlagen mit personenbezogenen Daten werden – sofern überhaupt erforderlich – in verschlossenen Ablagen aufbewahrt.
- Es erfolgt keine Speicherung von personenbezogenen Daten auf frei zugänglichen mobilen Datenträgern (z. B. USB-Sticks), außer in begründeten Einzelfällen und dann nur verschlüsselt.

4. Zugangskontrolle (Login zu IT-Systemen)

Ziel: Verhindern, dass Unbefugte auf IT-Systeme zugreifen können.

Maßnahmen u. a.:

- Nutzung individueller Benutzerkonten für alle administrativen Zugriffe (keine gemeinsamen Logins).
- SSH-Zugänge zum Server sind gehärtet:
  - Root-Login ist deaktiviert.
  - Passwort-Login ist für SSH deaktiviert; Anmeldung erfolgt ausschließlich mit SSH-Schlüsseln.
- Starke Passwortrichtlinien für alle weiteren Dienste (z. B. E-Mail, Admin-Portale), Nutzung eines Passwortmanagers.
- Nutzung von Mehr-Faktor-Authentifizierung (MFA), soweit vom jeweiligen Dienst (z. B. Mail- oder Cloud-Anbieter) unterstützt.
- Endgeräte verfügen über eine automatische Sperre nach Inaktivität (Bildschirmsperre).

5. Zugriffskontrolle (Berechtigungen innerhalb der Systeme)

Ziel: Sicherstellen, dass nur befugte Personen und nur im erforderlichen Umfang auf personenbezogene Daten zugreifen können.

Maßnahmen u. a.:

- Prinzip der Erforderlichkeit („Need-to-know“): Zugriff auf Daten nur, soweit für die jeweilige Tätigkeit notwendig.
- Die Datenbank (PostgreSQL) ist nur aus dem internen Docker-Netzwerk erreichbar; direkte Zugriffe von außen sind nicht möglich.
- Admin-Oberflächen und Kundenportale sind durch individuelle Benutzerkonten (E-Mail + Passwort) geschützt; Passwörter werden nur gehasht gespeichert.
- Berechtigungen werden regelmäßig überprüft (z. B. bei Beendigung von Mandaten oder Zusammenarbeit mit Dienstleistern).

6. Weitergabe- und Übertragungskontrolle

Ziel: Schutz personenbezogener Daten bei Übermittlung, Transport oder Speicherung auf externen Systemen.

Maßnahmen u. a.:

- Zugriff auf die Website, Formulare, Preisliste und den Kundenbereich ausschließlich über HTTPS (TLS).
- E-Mail-Kommunikation erfolgt über die bei Hetzner betriebenen Mailserver; die Übertragung erfolgt per TLS, soweit von der Gegenstelle unterstützt.
- Nach und nach werden DNS-basierte Schutzmechanismen (z. B. SPF, optional DKIM/DMARC) eingerichtet, um die Authentizität von Absender-Domains zu unterstützen.
- Bei besonders schutzbedürftigen Inhalten (z. B. sensible Dokumente) wird – soweit praktikabel – bevorzugt der Kundenbereich bzw. ein gesicherter Upload/Download genutzt, statt klassischem Mail-Anhang.
- Unterauftragsverarbeiter (z. B. Hosting, E-Mail) werden sorgfältig ausgewählt und vertraglich auf ein angemessenes Schutzniveau verpflichtet.

7. Eingabekontrolle

Ziel: Nachvollziehbarkeit, welche personenbezogenen Daten wann und durch wen eingegeben, verändert oder gelöscht wurden.

Maßnahmen u. a.:

- Nutzung einer zentralen Datenbank (PostgreSQL) für Kunden-, Mandanten- und Vorgangsdaten; Änderungen werden strukturierter statt „verteilt in Dateien“ vorgenommen.
- Webformulare (z. B. Anfrage, Self-Service-Formular, Kundenbereich) schreiben in klar definierte Tabellen mit Zeitstempeln.
- Log- und Protokollfunktionen der Anwendung und des Webservers werden genutzt, um technische Vorgänge nachvollziehen zu können (z. B. Fehlversuche, Statuscodes).
- Wesentliche Änderungen an Stammdaten (z. B. Kontaktdaten, Konditionen) werden nachvollziehbar dokumentiert.

8. Auftragskontrolle / Unterauftragsverhältnisse

Ziel: Sicherstellen, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

Maßnahmen u. a.:

- Verarbeitung personenbezogener Daten ausschließlich auf Grundlage der schriftlichen bzw. elektronischen Weisungen des Verantwortlichen (AVV, Einzelfallanweisungen).
- Abschluss bzw. Dokumentation von AVVs bzw. Auftragsverarbeitungsverhältnissen mit Unterauftragsverarbeitern (z. B. Hetzner Online GmbH als Hosting- und E-Mail-Provider).
- Keine eigene Nutzung oder Weitergabe von Daten zu eigenen Zwecken der Auftragsverarbeiterin.
- Änderungen an Unterauftragsverarbeitern erfolgen nur im Rahmen der vertraglichen Vereinbarungen mit dem Verantwortlichen (Informations- und ggf. Mitbestimmungsrechte).

9. Verfügbarkeitskontrolle und Wiederherstellbarkeit

Ziel: Schutz vor Verlust, Zerstörung und unbeabsichtigter Veränderung personenbezogener Daten.

Maßnahmen u. a.:

- Regelmäßige Backups der Datenbank:
  - Erstellung von Sicherungen (z. B. mittels pg_dump) in ein vom Produktivbetrieb getrenntes Backup-Verzeichnis auf dem Server.
  - Backups werden mit angemessener Aufbewahrungsdauer (mindestens mehrere Wochen, anpassbar nach Weisung des Verantwortlichen) vorgehalten.
- Die Anwendung läuft in Docker-Containern; Dienste können bei Bedarf reproduzierbar neu gestartet bzw. von einem frischen Container-Image aufgebaut werden.
- Einsatz von Server-Monitoring und Protokollanalyse (z. B. Docker-Logs, Systemjournale), um Unregelmäßigkeiten frühzeitig zu erkennen.
- Sicherheitsupdates des Betriebssystems und der eingesetzten Software (insb. Node.js, Datenbank, Caddy) werden regelmäßig eingespielt.
- Es bestehen dokumentierte Schritte zur Wiederherstellung der Anwendung (Code aus Versionsverwaltung, Konfiguration, Datenbank-Import).

10. Trennungskontrolle

Ziel: Sicherstellen, dass Daten zu unterschiedlichen Zwecken getrennt verarbeitet werden.

Maßnahmen u. a.:

- Strukturelle Trennung unterschiedlicher Datenkategorien in der Datenbank (z. B. Kundenstammdaten, Angebots-/Rechnungsdaten, Upload-Dokumente, Protokolle).
- Der Kundenbereich ist logisch vom Admin-Bereich getrennt; Kund:innen haben nur Zugriff auf ihre eigenen Daten (z. B. Rechnungen, Übergabeprotokolle, eigene Uploads).
- Test- und Entwicklungsumgebungen werden von produktiven Daten getrennt; produktive personenbezogene Daten werden nicht zu Testzwecken verwendet, außer nach ausdrücklicher Weisung und mit angemessener Anonymisierung/Pseudonymisierung.

11. Schutz vor unbefugten Zugriffsversuchen (Netzwerksicherheit)

Ziel: Reduzierung des Risikos automatisierter Angriffe und unbefugter Zugriffe.

Maßnahmen u. a.:

- Einsatz eines Reverse Proxy (Caddy) vor der Web-Anwendung; nur HTTP(S)-Ports sind von außen erreichbar.
- Begrenzung offener Ports auf das technisch Notwendige (z. B. SSH, HTTPS).
- Einsatz von Fail2Ban auf dem Server zur automatischen Sperrung von IP-Adressen bei wiederholten fehlgeschlagenen SSH-Anmeldeversuchen.
- Protokollierung von Anmeldeversuchen und Sperrungen; regelmäßige Überprüfung der Logfiles auf Auffälligkeiten.
- Nutzung sicherer Standardkonfigurationen (z. B. Deaktivierung unsicherer Protokolle, bevorzugt aktuelle TLS-Versionen).

12. Datenschutzfreundliche Technikgestaltung & Voreinstellungen

Ziel: Umsetzung der Anforderungen aus Art. 25 DSGVO („Privacy by Design“ / „Privacy by Default“).

Maßnahmen u. a.:

- Datenminimierung: Es werden nur solche Daten erhoben, die für die Vertragsdurchführung bzw. das jeweilige Verfahren (z. B. Angebot, Onboarding, laufende Zusammenarbeit) erforderlich sind.
- Formulare (Self-Service, Kontakt, Buchung) werden so gestaltet, dass Pflichtfelder klar erkennbar sind und keine unnötigen Angaben erzwungen werden.
- Standardmäßig werden keine personenbezogenen Daten zu Marketingzwecken verarbeitet, die nicht für die laufende Geschäftsbeziehung erforderlich sind – es sei denn, es liegt eine gesonderte Einwilligung vor.
- Lösch- und Aufbewahrungsfristen richten sich nach gesetzlichen Vorgaben (z. B. handels- und steuerrechtliche Pflichten) und den Weisungen des Verantwortlichen; darüber hinaus werden Daten gelöscht oder anonymisiert, sobald sie für die Zwecke der Verarbeitung nicht mehr erforderlich sind.

13. Regelmäßige Überprüfung, Bewertung und Anpassung

Ziel: Sicherstellen, dass die TOMs dem Stand der Technik und dem Risikoprofil entsprechen.

Maßnahmen u. a.:

- Regelmäßige (mindestens jährliche oder anlassbezogene) Überprüfung der TOMs, insbesondere bei:
  - Einführung neuer Systeme oder Prozesse,
  - Änderungen der gesetzlichen Anforderungen,
  - Sicherheitsvorfällen oder relevanten Beinahe-Vorfällen.
- Fortlaufende Pflege der Systemumgebung (Updates, Log-Checks, Prüfung von Diensten).
- Dokumentation wesentlicher Änderungen an der Infrastruktur (z. B. neue Unterauftragsverarbeiter, Umzug auf andere Server, neue Module im Kundenbereich).
- Bei Sicherheitsvorfällen wird der Verantwortliche unverzüglich nach Maßgabe der AVV informiert; es werden Ursachen analysiert und Korrekturmaßnahmen ergriffen.

14. Anpassungsvorbehalt

Die beschriebenen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung der organisatorischen Abläufe.

Die Auftragsverarbeiterin ist berechtigt, gleichwertige oder höhere Maßnahmen einzusetzen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Verantwortlichen auf Wunsch zur Verfügung gestellt.