# Technische und organisatorische Maßnahmen (TOM)

nach Art. 32 DSGVO – Anlage 2 zum Vertrag über die Auftragsverarbeitung

Version 2026-11 · Stand 06.11.2026

pronetic trifft die nachfolgend beschriebenen Maßnahmen, um bei der Verarbeitung personenbezogener Daten im Auftrag ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst; das Schutzniveau wird dabei nicht unterschritten (§ 8 AV-Vertrag).

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

**1.1 Zutrittskontrolle** – Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

- Hosting-, E-Mail- und Datenbankdaten der Kunden werden in Rechenzentren der Unterauftragsverarbeiter in Deutschland verarbeitet; weitere Verarbeitungsorte einzelner Unterauftragsverarbeiter, auch in Drittländern (z. B. Plattform für die Website-Wartung, KI-Dienste), ergeben sich aus Anlage 3. Die Rechenzentren verfügen nach eigenen Angaben über mehrstufige Zutrittskontrollen, Videoüberwachung, Einbruchmeldeanlagen, Protokollierung von Zutritten und Besucherregelungen; pronetic lässt sich entsprechende Nachweise (z. B. Zertifikate nach ISO/IEC 27001) vorlegen.
- In den Büroräumen von pronetic werden keine Server mit Kundendaten betrieben.
- Büroräume: verschlossene Türen außerhalb der Anwesenheit, dokumentierte Schlüsselvergabe, Besucher nur in Begleitung.

**1.2 Zugangskontrolle** – Schutz vor unbefugter Nutzung von Systemen

- Persönliche Benutzerkonten; keine gemeinsam genutzten Konten für Beschäftigte.
- Passwortrichtlinie (mindestens 12 Zeichen, keine Wiederverwendung); Zugangsdaten werden nur verschlüsselt abgelegt.
- Zwei-Faktor-Authentisierung für administrative Zugänge (Hosting-Verwaltung, Registrar, E-Mail-Verwaltung, Fernwartungskonto).
- Administrative Zugriffe auf Server nur über verschlüsselte Verbindungen (z. B. SSH mit Schlüsselauthentisierung, TLS).
- Automatische Bildschirmsperre; Festplattenverschlüsselung auf Notebooks und Arbeitsplatzrechnern.
- Aktuelle Betriebssysteme, Firewall und Virenschutz auf allen Endgeräten.
- Sperrung von Zugängen beim Ausscheiden von Beschäftigten oder freien Mitarbeitern.

**1.3 Zugriffskontrolle** – Zugriff nur auf die jeweils berechtigten Daten

- Berechtigungen nach dem Prinzip der minimalen Rechte (need to know); administrative Rechte nur für dafür vorgesehene Personen.
- Zugangsdaten von Kunden werden ausschließlich verschlüsselt und mit beschränktem Zugriff gespeichert und nur bei Bedarf genutzt.
- Protokollierung administrativer Zugriffe, soweit die eingesetzten Systeme dies unterstützen.
- Datenschutzgerechte Vernichtung von Datenträgern (nach DIN 66399) und Papierunterlagen.

**1.4 Trennungskontrolle** – getrennte Verarbeitung für unterschiedliche Zwecke

- Mandantentrennung: getrennte Hosting-Konten, Datenbanken und Postfächer je Kunde.
- Trennung von Entwicklungs-, Test- und Produktivumgebungen; Testdaten werden, soweit möglich, anonymisiert oder pseudonymisiert.
- Trennung der Kundendaten von den eigenen Geschäftsdaten von pronetic.

**1.5 Pseudonymisierung und Verschlüsselung** (Art. 32 Abs. 1 lit. a DSGVO)

- Verschlüsselte Übertragung (HTTPS/TLS für Websites, Verwaltungsoberflächen und Webmail; TLS für SMTP, IMAP und POP3).
- TLS-Zertifikate für alle betriebenen Websites.
- Fernwartung ausschließlich über Ende-zu-Ende-verschlüsselte Verbindungen.
- Pseudonymisierung bei Analysen und Tests, soweit für den Zweck möglich.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

**2.1 Weitergabekontrolle** – Schutz bei Übertragung und Transport

- Übermittlung personenbezogener Daten ausschließlich über verschlüsselte Verbindungen.
- Keine Übermittlung von Zugangsdaten oder besonders schutzbedürftigen Daten per unverschlüsselter E-Mail oder Messenger.
- Mobile Datenträger werden nur verschlüsselt eingesetzt.

**2.2 Eingabekontrolle** – Nachvollziehbarkeit von Eingaben und Änderungen

- Nachvollziehbarkeit durch persönliche Benutzerkonten.
- Protokollierung durch die Hosting-Plattform (Server- und Zugriffsprotokolle) sowie, soweit verfügbar, Änderungsprotokolle der Anwendungen.
- Dokumentation von Wartungs- und Supporteinsätzen (Leistungsnachweise, Tickets).

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

**3.1 Verfügbarkeitskontrolle** – Schutz vor zufälliger Zerstörung oder Verlust

- Rechenzentren mit redundanter Strom- und Klimaversorgung, unterbrechungsfreier Stromversorgung, Notstrom sowie Brandmelde- und Löschtechnik (Unterauftragsverarbeiter).
- Regelmäßige Datensicherungen der Hosting-Plattform; zusätzliche Sicherungen im Rahmen gebuchter Wartungsleistungen auf der Hosting-Plattform in Deutschland; die Wartungsplattform von WPMU DEV speichert keine Datensicherungen.
- Regelmäßige Aktualisierung von Systemen und Anwendungen (Patch-Management).
- Schutz vor Schadsoftware, Spam- und Virenfilter für E-Mails, Schutz vor Überlastungsangriffen durch den Rechenzentrumsbetreiber.
- Überwachung der Verfügbarkeit betreuter Websites im Rahmen gebuchter Wartungsleistungen.

**3.2 Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DSGVO)

- Dokumentierte Verfahren zur Wiederherstellung aus Datensicherungen; regelmäßige Wiederherstellungstests.
- Notfall- und Eskalationskontakte zu den Unterauftragsverarbeitern.
- Festgelegter Ablauf für Sicherheitsvorfälle einschließlich Meldung an betroffene Auftraggeber (möglichst innerhalb von 24 Stunden).

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) und mindestens jährliche Überprüfung dieser Maßnahmen.
- Verpflichtung aller Beschäftigten und freien Mitarbeiter auf Vertraulichkeit und Datenschutz, bei Bedarf auch auf § 203 StGB; regelmäßige Sensibilisierung und Schulung.
- Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) bei der Einrichtung von Systemen.

- Prozess für Datenschutzverletzungen (Erkennen, Bewerten, Dokumentieren, Melden).

### 5. Auftragskontrolle

- Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern; sorgfältige Auswahl und regelmäßige Prüfung der Nachweise.
- Dokumentierte Weisungen der Auftraggeber; Ausführung von Arbeiten nur im Rahmen des Auftrags.
- Fernwartung nur nach Freigabe durch den Auftraggeber im Einzelfall oder nach vereinbartem unbeaufsichtigtem Zugriff; Protokollierung der Verbindungen.
- Keine Verarbeitung personenbezogener Kundendaten in KI-Diensten Dritter, die nicht als Unterauftragsverarbeiter aufgeführt oder vom Auftraggeber angewiesen sind; keine Nutzung von Kundendaten zum Training von KI-Modellen.
- Regeln für mobiles Arbeiten: nur verschlüsselte Geräte, Sichtschutz, keine Ablage von Kundendaten auf privaten Geräten.