Dokumentation des Schutz-Niveaus der SaaS-Plattform safetytron.com

Anlage 2 zum Nutzungsvertrag über die SaaS-Plattform safetytron.com
Anlage zum Auftragsverarbeitungsvertrag nach § 3 Abs. 3 AVV
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

SafetyTron — Inhaber Benedict Schwing
Hammer Landstraße 48 · 20537 Hamburg · `info@safetytron.com`
Stand: 20.08.2026 · Fassung 2

Vorwort

Dieses Dokument trägt den Titel **„Dokumentation des Schutz-Niveaus der SaaS-Plattform safetytron.com"**. Es ist **Anlage 2 zum Nutzungsvertrag** und zugleich die nach **§ 3 Abs. 3 des Auftragsverarbeitungsvertrages (AVV)** vereinbarte Beschreibung der technischen und organisatorischen Maßnahmen. Es wird mit dem Abschluss des AVV als Anlage vereinbart.

Es beschreibt die technischen und organisatorischen Maßnahmen, die der Anbieter zum Schutz der im Auftrag des Kunden verarbeiteten personenbezogenen Daten getroffen hat. Damit erfüllt es die Anforderung des **Art. 28 Abs. 3 Satz 2 Buchst. c in Verbindung mit Art. 32 DSGVO**, wonach der Auftragsverarbeiter die von ihm ergriffenen Maßnahmen gegenüber dem Verantwortlichen darzulegen hat.

Mit Abschluss des AVV bestätigt der Kunde, dass er dieses Schutz-Niveau zur Kenntnis genommen und geprüft hat und dass er die nachfolgend beschriebenen Maßnahmen für die von ihm über die Plattform verarbeiteten personenbezogenen Daten als **angemessen und ausreichend im Sinne des Art. 32 Abs. 1 DSGVO** ansieht. Die Bestätigung ist am Ende dieses Dokuments gesondert ausgewiesen.

Die Darstellung folgt den drei Ebenen, auf denen die Plattform betrieben wird:

Ebene	Gegenstand	Verantwortung
1	Rechenzentrum — Gebäude, Zutritt, Strom, Kühlung, Brandschutz	IONOS SE und deren Rechenzentrumspartner
2	Server- und Cloud-Plattform — Virtualisierung, Netz, Speicher	IONOS SE
3	Anwendung — Programmierung, Rechte, Datentrennung	SafetyTron (Anbieter)

---

1 Prüfmaßstab und herangezogene Standards

Die Maßnahmen orientieren sich an den folgenden anerkannten Standards. Die Gliederung dieses Dokuments folgt den Schutzzielen des Art. 32 Abs. 1 DSGVO.

Standard	Bedeutung	Ebene
Art. 32 DSGVO	Gesetzlicher Maßstab: Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit, regelmäßige Überprüfung	1 – 3

Standard	Bedeutung	Ebene
ISO/IEC 27001	Managementsystem für Informationssicherheit; die eingesetzten Rechenzentren und die IONOS-Cloud-Plattform sind zertifiziert	1 – 2
ISO 9001	Qualitätsmanagement; Zertifizierung des Rechenzentrums Frankfurt 1	1
BSI C5 (Cloud Computing Compliance Criteria Catalogue)	Testat des Bundesamts für Sicherheit in der Informationstechnik für Cloud-Dienste; von IONOS für die Server-Plattform ausgewiesen	2
BSI IT-Grundschutz	Methodik des BSI; von IONOS für die Server-Plattform ausgewiesen	2
Tier-Klassifizierung (Uptime Institute)	Klassifizierung der Ausfallsicherheit von Rechenzentren	1 – 2
OWASP Top 10	Branchenüblicher Katalog der häufigsten Sicherheitsrisiken von Webanwendungen; Maßstab für die Entwicklung der Anwendung	3

> **Abgrenzung.** Die genannten Zertifizierungen und Testate beziehen sich auf die Rechenzentren und die Cloud-Plattform der IONOS SE. Der Anbieter selbst ist als Einzelunternehmen **nicht** nach ISO/IEC 27001 zertifiziert. Für die von ihm verantwortete Ebene 3 (Anwendung) gilt der OWASP-Katalog als Entwicklungs- und Prüfmaßstab. Diese Abgrenzung wird hier ausdrücklich offengelegt, damit der Kunde seine eigene Bewertung nach Art. 32 Abs. 1 DSGVO auf zutreffender Grundlage vornehmen kann.

---

2 Ebene 1 — Rechenzentren

Die Plattform wird **ausschließlich in Rechenzentren innerhalb der Bundesrepublik Deutschland** betrieben. Eine Verarbeitung oder Speicherung personenbezogener Daten außerhalb der Europäischen Union findet nicht statt. Ein Zugriff durch Stellen außerhalb der EU ist nicht vorgesehen.

Für den deutschen Rechenzentrumsverbund weist IONOS die folgenden Standorte und Merkmale aus (Quelle: `cloud.ionos.de/rechenzentren`, abgerufen am 14.08.2026).

2.1 Rechenzentrum Frankfurt am Main 1 — Betreiber Equinix, Inc.

Kategorie	Merkmale
Physische Sicherheit	Sicherheitsglas-Schleusen · Wachpersonal im 24×7-Sicherheitsdienst · 24×7-Überwachungssystem · Kartenlesegeräte zur Zugangskontrolle · biometrische Identifizierungssysteme · Einbruchmeldetechnik · Videoüberwachung
Standards / SLA	Weltweites Service Level Agreement: mehr als **99,999 %** Verfügbarkeit der Stromversorgung · mehr als **99,99 %** Verfügbarkeit der Klimatisierung · mehr als **99,99 %** Verfügbarkeit für Cross Connect
Zertifizierung	**ISO/IEC 27001** (Informationssicherheit) · **ISO 22301** (Betriebskontinuität) · **ISO 9001** (Qualitätsmanagement)
Netzwerk	Proprietäres Überkopf-Verkabelungssystem mit mehrstufigem Leiterhalter · Cross Connects über Single-Mode- und Multi-Mode-Glasfaser (62,5 und 50 µm), CAT5, CAT6, CAT5 (T1), CAT3 (POTS) · Metro Connect Managed Ethernet · Equinix Connect mit Multi-Homing

Kategorie	Merkmale
Stromversorgung	2 Energiezuleitungen, zum Ring verbunden · Eingangsspannung 10 kV · vier Leistungstransformatoren mit je 2.500 kVA · USV: 4 × 1.800 kVA in **N+1** (2N auf Anfrage) · Notstrom: **8 Dieselgeneratoren** mit zusammen 12.800 kVA in N+1 (2N auf Anfrage) · geschützte Beleuchtung, 300 Lux · 3–6 kVA je Cabinet
Kühlung	Kühlkapazität 1,5 kW/m² (5.119 BTU/h) · Zentrifugalkühler mit 6.840 kW

2.2 Rechenzentrum Frankfurt am Main 2 — Betreiber Digital Realty

Kategorie	Merkmale
Physische Sicherheit	24/7 besetzter Sicherheitsempfang · 24/7 gesicherter Zugang mit **Zwei-Faktor-Authentifizierung und amtlichem Lichtbildausweis** · hochqualifiziertes Sicherheitspersonal rund um die Uhr vor Ort · 24/7 kontrollierter Zugang · 24/7 Kundenservice-Support
Standards / SLA	Verfügbarkeit **99,999 %** · 100 % Strom aus erneuerbaren Quellen · modulare Architektur zur Optimierung der Energieeffizienz (PUE) · Betrieb nach höchsten Energieeffizienzstandards
Netzwerk	Mehrfache Anbindungen · Metro-Connect-Uplinks (Managed Wave und Dark Fiber) zu allen Digital-Realty-Rechenzentren in Frankfurt · Zugang zu über 700 Carriern, NSPs, IX-Providern und ISPs · **redundante Meet-Me-Räume** · ServiceFabric™-Plattform · strukturierte Verkabelung und Cross-Connects
Stromversorgung	16.200 kW IT-Leistung (2,0 kW je m²) · Energiezufuhr über interne 10-kV/110-kV-Umspannstation · **N+1** Dieselgenerator-Backup mit SLA für Kraftstofflieferung · **48 Stunden Kraftstoffbevorratung** gemäß SLA · USV in Hexaload- oder Triload-Topologie mit **2N-redundanter** Stromversorgung · Verfügbarkeit bis zu 99,999 % · bis zu 30 kW je Rack
Brandschutz und Klimatisierung	Fortschrittliche **Frühraucherkennung (VESDA)** in allen Kundenräumen · **Stickstofflöschsystem** · Brandwände nach **F90/F120** · Raumtemperatur und Luftfeuchtigkeit nach ASHRAE-Standard · mindestens **N+1** CRAC-Redundanz je Raum · Überdruckbelüftung in Kunden- und Technikräumen · redundantes Kaltwasserversorgungsnetz · **24/7-Monitoring aller Infrastrukturen** (Kühlung, Lüftung, CRAC, Brandmelder, Generatoren, USV)

2.3 Rechenzentrum Berlin — Betreiber IONOS

Kategorie	Merkmale
Physische Sicherheit	Brandschutzzonen · Brandfrüherkennung · Feuerlöschanlage
Standards / SLA	**Tier-Klassifizierung Tier III** · Verfügbarkeit **99,99 % p. a.**
Zertifizierung	**ISO/IEC 27001**
Netzwerk	Redundante 100-GB-Internet-Uplinks (2 × 100 GB WAN-Uplink) · 1 × 1 GB Out-of-Band-Uplink als Notfall-Ausfallsicherung
Stromversorgung	Eine Stromeinspeisung · Batteriepuffer · A/B-System mit **2N-USV-Redundanz** · Notstromdiesel mit **N+1**-Redundanz
Kühlung	Redundante Klimatisierung · Kaltgangeinhausung, Einblastemperatur 23 °C

2.4 Gemeinsame Aussagen des Betreibers

IONOS betreibt über 30 Rechenzentren weltweit, wobei die Rechenzentren in Deutschland im Mittelpunkt stehen. Diese sind nach modernsten Standards errichtet, arbeiten klimaneutral und werden professionell administriert. Alle Daten der IONOS-Kunden werden dadurch DSGVO-konform und mit erhöhtem Schutz gegenüber dem US CLOUD Act verarbeitet. Die Rechenzentren sind georedundant ausgelegt.

3 Ebene 2 — Server- und Cloud-Plattform

Die Anwendung läuft auf einem **dedizierten virtuellen Server der Produktlinie IONOS VPS+**. Für diese Plattform weist IONOS die folgenden Merkmale aus (Quelle: `ionos.de/server/vps`, abgerufen am 14.08.2026).

Bereich	Merkmal
Verfügbarkeit / SLA	Über **99,99 % Verfügbarkeit**, erreicht durch Infrastruktur-Redundanzen und intelligente Systemarchitekturen
Rechenzentrumsstandard	**Tier-IV-Zertifizierung** · 31 Rechenzentren weltweit · 100 % grüner Strom
Zertifizierungen und Testate	**ISO 27001** · **BSI C5-Testat** · **IT-Grundschutz des BSI**
Datenschutz	**100 % DSGVO-konform**; für SafetyTron ausschließlich deutsche Standorte gebucht
Angriffsabwehr	**Aktiver DDoS-Schutz** gegen böswillige Überlastung · individualisierbare **Firewall** mit individuellem Firewall-Management · IPS/IDS
Zugang	Verschlüsselter Remote-Zugang
Speicher	SSD-NVMe-Speichersysteme · High-Speed-Images als Point-in-Time-Snapshots · optionaler Backup-Service
Netzwerk	Unbegrenzter Traffic mit bis zu 1 Gbit/s · IPv4- und IPv6-Dual-Stack
Betreuung	24/7-Experten-Support mit persönlichem Berater

> **Hinweis zu den Verfügbarkeits- und Tier-Angaben.** Die Werte in den Abschnitten 2 und 3 sind die vom Betreiber je Standort beziehungsweise je Produktlinie veröffentlichten Angaben und stammen aus unterschiedlichen Quellen. Sie stehen nebeneinander und sind nicht gegeneinander aufzurechnen. Maßgeblich für das Verhältnis zwischen Anbieter und Kunde ist allein die in § 5 der AGB zugesagte Verfügbarkeit.

3.1 Konkrete Ausprägung bei SafetyTron

Merkmal	Umsetzung
Serverstandort	Deutschland (IONOS-Rechenzentrumsverbund, siehe Abschnitt 2)
Betriebssystem	Ubuntu Linux 24.04 LTS mit Sicherheitsaktualisierungen des Distributors
Server-Verwaltung	Plesk-Administrationsoberfläche, ausschließlich für den Anbieter zugänglich
Webserver	nginx mit HTTP/2 und HTTP/3
Anwendungslaufzeit	PHP 8.3 (aktive Sicherheitspflege durch die PHP Group)
Datenbank	MariaDB, gebunden an die lokale Schleife `127.0.0.1` — **kein Zugang aus dem Netz**
Administrativer Zugang	Ausschließlich über SSH mit **Public-Key-Verfahren** (ed25519); kein Passwort-Login
Trennung der Systeme	Getrennte Datenbanken für Anwendungsdaten, kaufmännische Daten und Lernplattform
Ablage von Zugangsdaten	Alle Zugangsdaten und Schlüssel liegen in Konfigurationsdateien **außerhalb des Web-Verzeichnisses** und sind über das Internet nicht abrufbar

4 Ebene 3 — Anwendung

Die nachfolgenden Maßnahmen betreffen die vom Anbieter selbst entwickelte Anwendung. Sie sind nach den Schutzzielen des Art. 32 Abs. 1 DSGVO gegliedert.

4.1 Vertraulichkeit

4.1.1 Zutrittskontrolle

Der physische Zutritt zu den Systemen ist ausschließlich über die in Abschnitt 2 beschriebenen Rechenzentrumsmaßnahmen möglich. Der Anbieter betreibt keine eigene Serverhardware und unterhält keine Räume, in denen personenbezogene Daten des Kunden physisch vorgehalten werden.

4.1.2 Zugangskontrolle — wer sich anmelden darf

Maßnahme	Umsetzung
Zentrale Anmeldung	Die Anmeldung erfolgt ausschließlich über einen eigenbetriebenen **Identitätsdienst (Authentik)** nach dem Standard **OpenID Connect**. Die Anwendung selbst nimmt im Regelbetrieb keine Passwörter entgegen.
Anmeldeverfahren	**Authorization-Code-Flow** mit vertraulichem Client. Bei jeder Anmeldung werden ein `state`- und ein `nonce`-Wert aus einem **kryptografisch sicheren Zufallsgenerator** erzeugt und beim Rücksprung geprüft; dies verhindert untergeschobene Anmeldungen. Der Austausch des Codes gegen das Zugangstoken findet **Server-zu-Server** statt, das Client-Geheimnis verlässt den Server nicht.
Passwortspeicherung	Wo im Ausnahmefall lokale Passwörter bestehen (Notfallzugänge), werden sie ausschließlich als **Hash nach dem bcrypt-Verfahren** gespeichert (`password_hash`/`password_verify`). Klartext-Passwörter werden zu keinem Zeitpunkt gespeichert.
Bestätigung der E-Mail-Adresse	Eine Anmeldung ist erst möglich, nachdem der Nutzer seine E-Mail-Adresse über einen zugesandten Bestätigungslink verifiziert hat.
Sitzungsverwaltung	Nach jeder erfolgreichen Anmeldung wird die Sitzungskennung **neu vergeben** (`session_regenerate_id`), womit das Übernehmen einer vorab gesetzten Sitzung ausgeschlossen ist.
Sitzungs-Cookies	Alle Sitzungs-Cookies sind mit den Merkmalen **`Secure`** (nur über verschlüsselte Verbindungen), **`HttpOnly`** (kein Zugriff durch Skripte im Browser) und **`SameSite`** (kein Mitsenden bei fremdinitiierten Aufrufen) versehen.
Sitzungsdauer	Standardmäßig **eine Stunde** mit gleitender Verlängerung bei aktiver Nutzung; bei ausdrücklicher Wahl „Angemeldet bleiben" zwölf Stunden. Danach ist eine erneute Anmeldung erforderlich.
Abmeldung	Die Abmeldung beendet neben der Sitzung in der Anwendung auch die zentrale Sitzung beim Identitätsdienst.
Notfallzugang	Für den Fall eines Ausfalls des Identitätsdienstes besteht ein gesondert abgesicherter Notfallzugang („Break Glass"). Er ist auf ausdrücklich gekennzeichnete Notfallkonten beschränkt, liegt unter einem nicht öffentlich verlinkten Pfad und ist über den regulären Anmeldeweg nicht erreichbar.

4.1.3 Zugriffskontrolle — wer was tun darf

Der Zugriff wird über **drei voneinander unabhängige Prüfungen** gesteuert. Jede darf für sich allein ablehnen; nur wenn alle drei zustimmen, wird eine Aktion ausgeführt.

Prüfung	Frage	Umsetzung
1 — Mandant	Ist der Zugang des Kunden aktiv?	Prüfung des Mandantenstatus unmittelbar im Anmelde-Wächter. Gesperrte oder beendete Mandanten kommen nicht durch.
2 — Paket	Ist das Modul im gebuchten Paket enthalten?	Prüfung in der Initialisierung jedes Fachmoduls. Nicht gebuchte Module sind auch über die direkte Adresszeile nicht erreichbar.
3 — Rolle	Darf diese Person das?	Zentrale Rechte-Matrix mit acht Rollen über acht Bereiche und vier Stufen (`keine` < `lesen` < `schreiben` < `verwalten`).

Ergänzend gilt:

- Die Rolle wird bei **jeder** Prüfung **frisch aus der Datenbank** gelesen, nicht aus der Sitzung. Der Entzug von Rechten wirkt dadurch sofort und nicht erst nach Ablauf der Sitzung.
- Findet die Prüfung keine aktive Berechtigung, gilt die **niedrigste** Stufe. Die Anwendung fällt im Zweifel auf „nichts erlaubt" zurück, nicht auf „alles erlaubt".
- Für Gastzugänge greift zusätzlich eine **Umfangsprüfung**: Die Rolle entscheidet, ob eine Aktion erlaubt ist, ein gesondert geführter Zuweisungsbestand entscheidet, auf **welche einzelnen Datensätze** sie angewendet werden darf. Beide müssen zustimmen.
- Schreibende Zugriffe werden nach dem **Positivlisten-Prinzip** behandelt: Jede Übermittlung von Formulardaten gilt als Änderung und ist rechtepflichtig, solange sie nicht ausdrücklich als unkritisch gelistet ist. Eine vergessene Absicherung führt damit zur Ablehnung und nicht zu einer unbemerkten Lücke.
- Sämtliche Prüfungen laufen **auf dem Server**. Ausgeblendete Menüpunkte sind eine Bequemlichkeit für den Nutzer, keine Sicherheitsmaßnahme; ein direkter Aufruf der Adresse führt zur selben Ablehnung.

4.1.4 Trennungskontrolle — Trennung der Kundendaten

Maßnahme	Umsetzung
Mandantenkennung	Jeder Kunde erhält einen eigenen Mandanten. Sämtliche Datensätze tragen dessen Kennung.
Herkunft der Kennung	Die Mandantenkennung wird **ausschließlich aus der serverseitigen Sitzung** gelesen. Sie wird zu keinem Zeitpunkt aus Adresszeile, Formularfeld oder Cookie übernommen; ein Kunde kann sie also nicht setzen oder verändern.
Filterung	Jede lesende und schreibende Abfrage der Fachdaten enthält die Mandantenkennung als Bedingung.
Abweisung fremder Identitäten	Meldet sich eine Identität an, der kein Kundenzugang zugeordnet ist, wird die Sitzung verworfen statt mit unbestimmtem Mandanten fortgeführt.
Dateiablage	Hochgeladene Dateien werden je Mandant in getrennten Verzeichnissen abgelegt.

4.1.5 Weitergabekontrolle — Transportverschlüsselung

Maßnahme	Umsetzung
Verschlüsselung	Sämtliche Verbindungen zur Plattform sind mit **TLS** verschlüsselt.
Zugelassene Verfahren	Ausschließlich **TLS 1.2 und TLS 1.3**. Die veralteten Versionen TLS 1.0 und TLS 1.1 werden vom Server **abgewiesen** (am 14.08.2026 geprüft).
Erzwingung	Unverschlüsselte Aufrufe werden serverseitig mit einer dauerhaften Weiterleitung (HTTP 301) auf die verschlüsselte Adresse umgelenkt.

Maßnahme	Umsetzung
Zertifikate	Zertifikate einer öffentlichen, browserseitig anerkannten Zertifizierungsstelle; automatisierte Erneuerung.
Interner Datenverkehr	Datenbank und Identitätsdienst sind an die lokale Schleife des Servers gebunden. Dieser Verkehr verlässt den Server nicht.
E-Mail-Versand	Versand über authentifizierte, transportverschlüsselte SMTP-Verbindung. Für die Absenderdomain sind **SPF, DKIM und DMARC** eingerichtet.

4.1.6 Verschlüsselung gespeicherter Zugangsdaten

Von Kunden hinterlegte Zugangsdaten zu Drittsystemen (z. B. Buchhaltungs-Schnittstellen) werden **verschlüsselt gespeichert** (AES-256 im CBC-Modus mit je Datensatz neu erzeugtem Initialisierungsvektor). Der Schlüssel liegt außerhalb des Web-Verzeichnisses in der Serverkonfiguration.

4.2 Integrität

4.2.1 Schutz vor Einschleusung von Datenbankbefehlen

Sämtliche Datenbankzugriffe erfolgen über **vorbereitete Anweisungen mit gebundenen Parametern** (PDO Prepared Statements). Die Emulation vorbereiteter Anweisungen ist **abgeschaltet** (`ATTR_EMULATE_PREPARES = false`); die Trennung von Befehl und Daten findet damit im Datenbankserver selbst statt. Benutzereingaben werden zu keiner Stelle in einen Befehlstext eingesetzt. Dies adressiert Risiko **A03 „Injection"** des OWASP-Katalogs.

4.2.2 Schutz vor Skript-Einschleusung

Alle in der Oberfläche ausgegebenen Werte werden vor der Ausgabe **maskiert** (`htmlspecialchars`). Vom Nutzer stammender Text kann dadurch nicht als Programmanweisung im Browser eines anderen Nutzers ausgeführt werden (Cross-Site Scripting, OWASP **A03**).

4.2.3 Schutz vor unbeabsichtigtem Überschreiben

Datensätze, an denen mehrere Personen arbeiten können, tragen eine **Versionsnummer**. Beim Speichern wird geprüft, ob sich der Datensatz zwischenzeitlich geändert hat. Ist das der Fall, wird der Vorgang **abgebrochen und gemeldet**, statt die Änderung des anderen Nutzers stillschweigend zu überschreiben. Prüfprotokolle werden zusätzlich über eine gesonderte Schutzschicht geschrieben, die Eigentümerschaft und Mandant vor jeder Änderung prüft.

4.2.4 Eingabekontrolle und Protokollierung

Was wird protokolliert	Inhalt
Anmeldungen und Verwaltungsvorgänge im Mandanten	Zeitpunkt, Benutzer, Aktion, betroffener Datensatztyp und -bezug, IP-Adresse
Betreibervorgänge	Zeitpunkt, Benutzer, Aktion, betroffener Datensatz, IP-Adresse
Technische Fehler	Server-Fehlerprotokoll ohne personenbezogene Nutzdaten

Fehlermeldungen der Anwendung werden im Produktivbetrieb **nicht an den Browser ausgegeben** (`display_errors` abgeschaltet). Technische Einzelheiten, aus denen sich Rückschlüsse auf Aufbau oder Datenbestand ziehen ließen, verlassen den Server nicht.

4.3 Verfügbarkeit und Belastbarkeit

Maßnahme	Umsetzung
Infrastruktur	Redundanzen der Ebenen 1 und 2 (Strom, Kühlung, Netzanbindung, siehe Abschnitte 2 und 3)
Angriffsabwehr	DDoS-Schutz und Firewall der Plattform (Ebene 2)
Zugesagte Verfügbarkeit	Der Anbieter schuldet gegenüber dem Kunden eine Verfügbarkeit von **99 % im Monatsmittel** am Übergabepunkt (§ 5 AGB). Die darunterliegenden Plattform-Werte (99,99 % und besser) sind Merkmale der Infrastruktur, keine gesonderte Zusage des Anbieters.
Wartung	Planbare Arbeiten nach Möglichkeit außerhalb von 07:00 bis 20:00 Uhr, mit Ankündigung mindestens 24 Stunden vorher
Aktualisierungen	Sicherheitsaktualisierungen des Betriebssystems und der Laufzeitumgebung werden zeitnah eingespielt
Notabschaltung	Der Zugang kann bei akuter Gefahr für Systeme oder Daten unverzüglich unterbrochen werden; der Kunde wird nachträglich unverzüglich informiert

4.4 Wiederherstellbarkeit

Maßnahme	Umsetzung
Rhythmus	**Wöchentliche Sicherung** des Gesamtsystems (Datenbanken und Dateien)
Aufbewahrung	Es werden die **letzten zwölf Sicherungsstände** vorgehalten; das entspricht einem rückwirkenden Zeitraum von rund einem Quartal
Zweck	Die Sicherungen dienen der Wiederherstellung des **Gesamtsystems**. Ein Anspruch auf Wiederherstellung einzelner vom Kunden gelöschter Datensätze besteht nicht (§ 11 Abs. 2 AGB)
Zusätzlich	Point-in-Time-Snapshots der Server-Plattform (Ebene 2)
Mitwirkung des Kunden	Der Kunde ist gehalten, für ihn wesentliche Daten — insbesondere Prüfprotokolle und Nachweise mit gesetzlicher Aufbewahrungspflicht — über die Exportfunktionen der Anwendung zusätzlich selbst zu sichern

4.5 Verfahren zur regelmäßigen Überprüfung

Maßnahme	Umsetzung
Funktionstests	Die Fachmodule werden blockweise nach festen, dokumentierten Testplänen geprüft; die Ergebnisse werden schriftlich festgehalten
Rechteprüfung	Die Rechte-Matrix wird gegen die tatsächlichen Datenbankwerte getestet; abweichende Auswahllisten werden auf eine gemeinsame Quelle zurückgeführt
Prüfung mit Anmeldung	Für geschützte Seiten besteht ein Prüfstand, der Sitzungen gezielt aufbaut und jede Seite in einem eigenen Prozess aufruft — auch gegen das Produktivsystem
Trennung der Umgebungen	Entwicklung und Produktivbetrieb laufen auf getrennten Systemen. Änderungen werden zuerst in der Entwicklungsumgebung geprüft
Anlassbezogene Prüfung	Sicherheitsrelevante Befunde werden dokumentiert und die betroffene Stelle wird systematisch im gesamten Bestand nachgezogen

---

5 Organisatorische Maßnahmen

Maßnahme	Umsetzung
Personenkreis	Der Anbieter ist ein Einzelunternehmen. Zugriff auf Systeme und Kundendaten hat ausschließlich der Inhaber.
Zweckbindung	Ein Zugriff auf Kundendaten erfolgt ausschließlich zur Erfüllung des Vertrages, zur Störungsbeseitigung oder auf ausdrückliche Weisung des Kunden.
Vertraulichkeit	Der Inhaber ist auf das Datengeheimnis verpflichtet. Werden künftig weitere Personen tätig, erfolgt deren Verpflichtung vor Aufnahme der Tätigkeit und vor jedem Zugriff.
Trennung der Rollen	Der Betreiberzugang (Verwaltungsoberfläche) und die Kundenzugänge sind getrennte Anwendungen mit getrennten Berechtigungen. Ein Betreiberkonto erhält in der Kundenanwendung keinen Zugang.
Unterauftragsverarbeiter	Der Einsatz von Unterauftragsverarbeitern — insbesondere für Hosting, E-Mail-Versand und Zahlungsabwicklung — richtet sich nach dem AVV und der dort geführten Liste.
Löschung	Nach Vertragsende bleiben die Daten 30 Tage in gesperrtem Zustand erhalten und werden danach endgültig gelöscht (§ 20 AGB). Gesetzliche Aufbewahrungspflichten des Anbieters bleiben unberührt.
Meldewege	Der Kunde erreicht den Anbieter für datenschutzrechtliche Anliegen und Sicherheitsvorfälle unter `info@safetytron.com`. Der Anbieter unterstützt den Kunden bei dessen Meldepflichten nach Art. 33 und 34 DSGVO.

---

6 Weiterentwicklung des Schutz-Niveaus

Der Anbieter entwickelt das Schutz-Niveau fortlaufend weiter. Vorgesehen sind unter anderem:

- Ausbau der HTTP-Sicherheitsmerkmale (HSTS, Content-Security-Policy, Frame- und Referrer-Vorgaben) für alle Anwendungsbereiche
- Angebot einer **Zwei-Faktor-Authentisierung** über den Identitätsdienst
- Ergänzende serverseitige Prüfung hochgeladener Dateien anhand des tatsächlichen Dateityps
- Begrenzung der Anmeldeversuche je Konto und Herkunft
- Automatisierte Auslagerung der Sicherungen auf ein zweites, getrenntes Ziel

Wesentliche Änderungen dieses Schutz-Niveaus teilt der Anbieter dem Kunden in Textform mit. Eine Absenkung des beschriebenen Niveaus ohne Zustimmung des Kunden findet nicht statt.

---

7 Bestätigung durch den Kunden

Der Kunde bestätigt mit Abschluss des Auftragsverarbeitungsvertrages, zu dem diese Anlage gehört:

- **(1)** Er hat die vorstehende **Dokumentation des Schutz-Niveaus der SaaS-Plattform safetytron.com** erhalten, zur Kenntnis genommen und geprüft.
- **(2)** Er hält die beschriebenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen für **angemessen und ausreichend im Sinne des Art. 32 Abs. 1 DSGVO**.

- **(3)** Ihm ist bekannt, dass die Verantwortung für die Auswahl der in die Plattform eingestellten Daten, für deren Rechtsgrundlage und für die Erfüllung der eigenen Pflichten als Verantwortlicher bei ihm liegt.

Die Bestätigung erfolgt zusammen mit dem Auftragsverarbeitungsvertrag. Nach **Art. 28 Abs. 9 DSGVO** genügt hierfür ein elektronisches Format; eine eigenhändige Unterschrift ist nicht erforderlich. Der Anbieter zeichnet Fassung, Wortlaut, Zeitpunkt und IP-Adresse der Bestätigung auf und stellt dem Kunden diesen Nachweis auf Anfrage zur Verfügung.

	Kunde (Verantwortlicher)	**Anbieter (Auftragsverarbeiter)**
Name	— Firma des Kunden —	SafetyTron — Inhaber Benedict Schwing
Bestätigt am	— noch nicht bestätigt —	20.08.2026
Nachweis	— wird bei der Bestätigung erzeugt —	Bereitstellung dieser Fassung

---

SafetyTron · Inhaber Benedict Schwing · Hammer Landstraße 48 · 20537 Hamburg
Dokumentenstand 20.08.2026 · Fassung 2 · Anlage 2 zum Nutzungsvertrag