Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

der IOS Solutions Services GmbH, Sprottauer Str. 25, 90475 Nürnberg (nachfolgend „IOS Solutions“)

Version 4.0 – Stand: 31.10.2026– Anlage zum Vertrag zur Auftragsverarbeitung (Anhang III) – ersetzt die Fassung vom 18.12.2025

1. Grundlagen

1.1 Geltungsbereich

Dieses Dokument beschreibt die Maßnahmen, mit denen IOS Solutions die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet, die es im Auftrag seiner Kunden verarbeitet. Es gilt für die Leistungen Managed und Unmanaged Server, vServer, Colocation, E-Mail-Hosting, Microsoft 365, Domains, Backup, IT-Support und Administration (remote und vor Ort) sowie Softwareentwicklung.

1.2 Risikobasierter Ansatz

Die Maßnahmen wurden unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ausgewählt (Art. 32 Abs. 1 DSGVO). Da IOS Solutions den Inhalt der auf Kundensystemen gespeicherten Daten nicht kennt, wird grundsätzlich von einem normalen bis hohen Schutzbedarf ausgegangen, einschließlich möglicher Daten nach Art. 9 DSGVO und Daten von Berufsgeheimnisträgern.

1.3 Abgrenzung der Verantwortung

Welche Maßnahmen IOS Solutions selbst trifft und welche dem Kunden obliegen, hängt von der gebuchten Leistung ab:

Bereich	Managed Server / vServer, E-Mail-Hosting, Backup	Unmanaged Server / vServer	Colocation
Rechenzentrum, Strom, Klima, physische Sicherheit	IOS Solutions (mit Hetzner)	IOS Solutions (mit Hetzner)	IOS Solutions (mit Hetzner)
Hardware, Virtualisierung, Netzwerk	IOS Solutions	IOS Solutions	Kunde (eigene Hardware); Netzanbindung IOS Solutions
Betriebssystem, Updates, Härtung	IOS Solutions	Kunde	Kunde
Anwendungen, Benutzer- und Rechteverwaltung	IOS Solutions bzw. nach Vereinbarung	Kunde	Kunde
Datensicherung	IOS Solutions (lokal und offsite)	Kunde, sofern kein Backup gebucht	Kunde
Verschlüsselung von Inhaltsdaten in Anwendungen	nach Vereinbarung	Kunde	Kunde

Für Microsoft 365 gelten ergänzend die Sicherheitsmaßnahmen von Microsoft; IOS Solutions verantwortet die sichere Administration des Tenants im Rahmen des Auftrags. Bei IT-Support und Administration vor Ort gelten die Maßnahmen dieses Dokuments für das Handeln der Mitarbeiter von IOS Solutions; im Übrigen gelten die Maßnahmen des Kunden.

IOS Solutions Services GmbH – Sprottauer Str. 25 – 90475 Nürnberg – Telefon: +49 (0)911-215371-0 – E-Mail: info@iossol.de

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

2.1 Zutrittskontrolle

Ziel: Unbefugten den Zutritt zu Räumen und Anlagen verwehren, in denen personenbezogene Daten verarbeitet werden.

Rechenzentrum

- Die Server von IOS Solutions sind ausschließlich im Rechenzentrum der Hetzner Online GmbH in Nürnberg, Sigmundstraße 135, in von IOS Solutions angemieteten Racks untergebracht.
- Der Rechenzentrumsbetreiber ist nach DIN EN ISO/IEC 27001:2022 zertifiziert.
- Zutritt zum Rechenzentrum erhalten nur Personal des Betreibers sowie namentlich hinterlegte Techniker von IOS Solutions; Zutritte werden protokolliert.
- Die Racks von IOS Solutions sind mit Schlössern (mechanisches Schloss) verschlossen. Für das gesamte Rechenzentrum gibt es Videoüberwachung, Vereinzelung und 24/7-Personal.

Büro Nürnberg, Sprottauer Str. 25

- Absicherung durch Alarmanlage und Videokameras; im Alarmfall werden die verantwortlichen Mitarbeiter automatisch alarmiert.
- Türen sind durch eine zentrale Schließanlage gesichert, Schlüssel werden dokumentiert ausgegeben.
- Besucher halten sich nur in Begleitung von Mitarbeitern in den Büroräumen auf.
- Der Raum, in dem die Offsite-Datensicherungen gespeichert werden, ist gesondert verschlossen.

2.2 Zugangskontrolle

Ziel: Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Jeder Administrator hat eine individuelle, persönliche Benutzerkennung; Sammel- oder Gruppenkonten werden für administrative Zugriffe nicht verwendet.
- **Multi-Faktor-Authentifizierung (MFA)** ist für alle zentralen Dienste eingerichtet, insbesondere für Verwaltungskonsolen (z. B. Virtualisierung, Microsoft-365-Partnerverwaltung, Domainverwaltung), das Support-System und die Fernwartungssoftware.
- Administrativer Zugang zu den Servern ist nur über das Netzwerk von IOS Solutions bzw. über verschlüsselte VPN-Verbindungen möglich.
- Kennwortrichtlinie in Anlehnung an das BSI-Grundschutzkompendium: ausreichende Länge (mind. 12 Zeichen) und Komplexität, keine Mehrfachverwendung, Wechsel bei Verdacht auf Kompromittierung; Verwendung eines Passwortmanagers.
- Für Serverzugänge werden vorrangig SSH-Schlüssel statt Kennwörtern eingesetzt.
- Automatische Bildschirmsperre an Arbeitsplätzen und Notebooks nach Inaktivität.
- Firewall-Schutz von Infrastruktur und Büronetz; nicht benötigte Dienste und Ports sind deaktiviert.
- Zugänge ausscheidender Mitarbeiter werden am letzten Arbeitstag gesperrt; Kennwörter und Schlüssel, die diese kannten, werden geändert.

2.3 Zugriffskontrolle

Ziel: Sicherstellen, dass Berechtigte nur auf die Daten zugreifen können, die ihrer Berechtigung unterliegen, und dass Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Es besteht ein Berechtigungskonzept nach dem Prinzip der minimalen Rechte (need to know); Berechtigungen werden regelmäßig überprüft.
- Auf Daten von Kunden wird nur zugegriffen, soweit dies für die beauftragte Leistung erforderlich ist.
- **Fernwartung:** Die Fernwartungssoftware ConnectWise Control wird von IOS Solutions selbst betrieben (on-premise); es besteht keine Abhängigkeit von einem Cloud-Dienst des Herstellers. Der Zugang ist durch MFA

IOS Solutions Services GmbH – Sprottauer Str. 25 – 90475 Nürnberg – Telefon: +49 (0)911-215371-0 – E-Mail: info@iossol.de

geschützt, Sitzungen werden protokolliert. Unbeaufsichtigte Zugriffe erfolgen nur, soweit mit dem Kunden vereinbart.

- Unmanaged Systeme: Zugriff nur über einen vom Kunden temporär bereitgestellten Zugang; der Kunde deaktiviert diesen nach Abschluss der Arbeiten.
- Datenträger werden vor Wiederverwendung oder Entsorgung nach DIN 66399 sicher gelöscht oder vernichtet.
- Notebooks und mobile Datenträger sind vollständig verschlüsselt (BitLocker).

2.4 Trennungskontrolle

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

- Physische oder logische Trennung der Kundensysteme: eigene virtuelle Maschinen je Kunde, Trennung von Netzwerksegmenten (VLAN).
- Getrennte Microsoft-365-Tenants je Kunde; getrennte Postfächer und Domains beim E-Mail-Hosting.
- Trennung von Entwicklungs-, Test- und Produktivumgebungen in der Softwareentwicklung.
- Berechtigungskonzept auf den Systemen.

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

- Administrative Zugriffe erfolgen ausschließlich über verschlüsselte Verbindungen (SSH, TLS 1.2 oder höher, VPN).
- Webdienste, Kundenportal und E-Mail-Dienste (IMAP, POP3, SMTP-Submission) sind nur verschlüsselt per TLS erreichbar; beim E-Mail-Transport zwischen Servern wird STARTTLS angeboten.
- Die wöchentliche Spiegelung der Datensicherungen vom Rechenzentrum ins Büro erfolgt über eine verschlüsselte Verbindung (VPN).
- Datensicherungen werden verschlüsselt gespeichert.
- Eine Pseudonymisierung von Inhaltsdaten erfolgt durch IOS Solutions nicht, da die Daten vom Kunden bestimmt werden; in der Softwareentwicklung werden vorrangig anonymisierte oder synthetische Testdaten verwendet.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

Ziel: Sicherstellen, dass Daten bei der Übertragung, beim Transport und bei der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und nachvollziehbar ist, wohin Daten übermittelt werden.

- Verschlüsselte Übertragungswege gemäß Ziffer 2.5.
- Bei der Verwaltung der Netzwerkhardware (Router, Switches) besteht eine technisch bedingte Zugriffsmöglichkeit auf übertragene Daten. Diese ist auf wenige geschulte Mitarbeiter beschränkt und dient ausschließlich dem technischen Betrieb; eine gezielte Auswertung personenbezogener Daten findet nicht statt.
- Physische Datenträger werden nur verschlüsselt bzw. persönlich oder als verfolgbare Sendung transportiert.
- Übermittlungen an Dritte erfolgen nur an die im AV-Vertrag (Anhang IV) genannten Unterauftragsverarbeiter oder auf dokumentierte Weisung des Kunden.

3.2 Eingabekontrolle

Ziel: Nachträglich prüfen können, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden.

- Administrative Zugriffe und Änderungen durch IOS Solutions werden protokolliert (Systemprotokolle, Sitzungsprotokolle der Fernwartung) und im Ticketsystem dokumentiert.

IOS Solutions Services GmbH – Sprottauer Str. 25 – 90475 Nürnberg – Telefon: +49 (0)911-215371-0 – E-Mail: info@iossol.de

- Protokolle werden 30 Tage aufbewahrt und vor unbefugter Veränderung geschützt.
- Die Eingabekontrolle für Inhaltsdaten in den Anwendungen des Kunden obliegt dem Kunden, sofern nicht anders vereinbart.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Ziel: Daten gegen zufällige Zerstörung oder Verlust schützen und die Systeme so auslegen, dass sie Belastungen und Störungen standhalten.

- **Rechenzentrum:** Nach dem Stand der Technik ausgestattet mit unterbrechungsfreier Stromversorgung und Notstrom, Klimatisierung, Brandfrüherkennung und -schutz sowie redundanter Netzanbindung (ISO/IEC 27001:2022-zertifizierter Betreiber).
- **Monitoring:** Überwachung von Verfügbarkeit, Ressourcen und Diensten mit Zabbix; automatische Alarmierung der zuständigen Techniker bei Störungen.
- **Datensicherung (Managed-Leistungen und gebuchtes Backup):** tägliche Sicherung; wöchentliche Spiegelung der Sicherungen vom Rechenzentrum in das räumlich getrennte Büro von IOS Solutions (Offsite-Kopie). Aufbewahrungsdauer: 360 Tage.
- **Patch-Management:** Sicherheitsupdates für betreute Systeme werden zeitnah innerhalb eines monatlichen Wartungsfensters eingespielt, kritische Sicherheitslücken vorrangig innerhalb von 72 Stunden.
- Spam- und Virenschutz für das E-Mail-Hosting; Virenschutz auf den Arbeitsplätzen von IOS Solutions.
- Redundante Auslegung kritischer Komponenten. Festplattensysteme sind ausnahmslos als RAID (redundant) ausgelegt. Ersatzsysteme (Switche, Router, Server) werden verfügbar gehalten.
- Für unmanaged Systeme und Colocation obliegt die Datensicherung dem Kunden; Backup, Firewall und Virenschutz können zusätzlich gebucht werden.

5. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Wiederherstellungen aus Datensicherungen werden regelmäßig getestet, mindestens quartalsweise stichprobenartig; die Tests werden dokumentiert.
- Es besteht ein Notfallplan mit Meldewegen, Zuständigkeiten, Wiederanlaufprioritäten und Handlungsanweisungen für typische Szenarien (z. B. Hardwareausfall, Ransomware, Ausfall des Rechenzentrums).
- Für die Wiederherstellung stehen sowohl Sicherungen im Rechenzentrum als auch die Offsite-Kopie im Büro zur Verfügung.

6. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

6.1 Datenschutz-Organisation

- Die Geschäftsführung trägt die Verantwortung für Datenschutz und Informationssicherheit. Ansprechpartner: Michael Hadlich, datenschutz@iossol.de.
- Eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht derzeit nicht (Art. 37 DSGVO, § 38 BDSG).
- Alle Mitarbeiter sind schriftlich auf die Vertraulichkeit (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO) sowie auf die Verschwiegenheit nach § 203 StGB verpflichtet und werden bei Eintritt und anschließend mindestens jährlich zu Datenschutz und Informationssicherheit geschult.
- Ein Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO) wird geführt.

6.2 Überprüfung und Verbesserung

- Diese Maßnahmen werden mindestens jährlich sowie anlassbezogen (z. B. bei neuen Leistungen, Sicherheitsvorfällen oder neuen Bedrohungen) überprüft und aktualisiert.

IOS Solutions Services GmbH – Sprottauer Str. 25 – 90475 Nürnberg – Telefon: +49 (0)911-215371-0 – E-Mail: info@iossol.de

- Regelmäßige Prüfung auf bekannte Schwachstellen der betreuten Systeme.
- Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung (Art. 25 DSGVO) werden bei neuen Leistungen und in der Softwareentwicklung berücksichtigt.

6.3 Umgang mit Sicherheitsvorfällen

- Sicherheitsvorfälle und Verdachtsfälle werden nach einem festgelegten Prozess erfasst, bewertet, eingedämmt und dokumentiert.
- Betroffene Kunden werden unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, informiert.
- Nach jedem Vorfall erfolgt eine Nachbereitung mit Ableitung von Verbesserungsmaßnahmen.

7. Auftragskontrolle

Ziel: Sicherstellen, dass im Auftrag verarbeitete Daten nur entsprechend den Weisungen des Kunden verarbeitet werden.

- Mit jedem Kunden wird ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO geschlossen; Weisungen werden in Textform dokumentiert.
- Unterauftragsverarbeiter werden sorgfältig ausgewählt (u. a. anhand von Zertifizierungen und TOM) und vertraglich auf dieselben Datenschutzpflichten verpflichtet; die Liste ist im Kundenportal abrufbar.
- Kunden haben ein Kontroll- und Prüfrecht nach Maßgabe des AV-Vertrags.
- Nach Vertragsende werden Daten nach Wahl des Kunden gelöscht oder zurückgegeben; die Löschung wird bestätigt.

Die technischen Möglichkeiten unterliegen einem stetigen Wandel. IOS Solutions passt die hier beschriebenen Maßnahmen dem Stand der Technik an, ohne das Schutzniveau zu unterschreiten. Mit Veröffentlichung einer neuen Fassung unter https://iossol.de/datenschutz verliert die vorliegende Fassung ihre Gültigkeit.

IOS Solutions Services GmbH – Sprottauer Str. 25 – 90475 Nürnberg – Telefon: +49 (0)911-215371-0 – E-Mail: info@iossol.de