Anlage 2 zum Vertrag über Auftragsverarbeitung

Technische und organisatorische Maßnahmen (TOM) im Sinne von Art. 32 DSGVO

Flowmium GmbH
Robert-Bosch-Str. 7
64293 Darmstadt

Allgemeines

Die Flowmium GmbH betreibt keine eigenen Datenverarbeitungsanlagen. Kundendaten werden im Rechenzentrum der centron GmbH in Hallstadt (Deutschland) gespeichert und verarbeitet. Wir verweisen auf die technischen und organisatorischen Maßnahmen der centron GmbH, die diesem Dokument beiliegen.

Flowmium betreibt ein ISMS nach ISO 27001 und ist seit dem 29.01.2024 zertifiziert.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Flowmium stellt sicher, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Dies geschieht durch:

- Elektronisches Türschloss zum Büro
- Abschließbare Fenster im Erdgeschoss
- Protokollierte Schlüsselverwaltung
- Dokumentierte Sicherheitsverfahren für Büros sowie sichere Bereiche und Betriebsmittel

1.2. Zugangskontrolle

Flowmium verhindert, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Dies geschieht durch:

- Login mit Benutzername und Passwort oder biometrische Verfahren
- 2-Faktor-Authentifizierung zu Server-, E-Mail- und Dokumentensystemen. Bei allen anderen Anwendungen, wenn möglich.
- Anti-Viren-Software auf Servern
- Anti-Viren-Software auf PCs/Notebooks
- Verschlüsselung von PCs/Notebooks
- Verschlüsselung von Smartphones
- Einsatz von Firewall und regelm. Aktualisierung
- Einsatz eines Intrusion Detection Systems (IDS)
- IT-Sicherheitsrichtlinie einschl. Passwortrichtlinie und Richtlinie zu aufgeräumtem Arbeitsplatz und leerem Bildschirm
- Richtlinie zu Mobilgeräten und mobilem Arbeiten einschl. Wahrung der Vertraulichkeit gegenüber unbefugten Personen, bei Gesprächen und dem Verbot öffentlicher WLAN-Netzwerke
- Anweisung zur Sperrung des PCs beim Verlassen des (Home-Office)Arbeitsplatzes
- Automatische Sperre des PCs bei Inaktivität
- Definierter Ablauf zur Löschung der Berechtigungen von ausgeschiedenen Mitarbeitern

1.3. Zugriffskontrolle

Flowmium gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

- Verschlüsselung der Datenbanken auf Dateiebene per TDE. Verschlüsselungsalgorithmus: AES256
- Einsatz eines Berechtigungskonzepts
- Minimale Anzahl an Administratoren
- Vergabe minimaler Berechtigungen
- Vernichtung von Datenträgern gemäß Richtlinie zur Entsorgung und Vernichtung
- Aktenvernichter mit Sicherheitsstufe P4

1.4. Trennungskontrolle

Flowmium gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies geschieht durch:

- Logische Trennung der personenbezogenen Daten für unterschiedliche Auftraggeber
- Trennung von Produktiv-, Test-, und Entwicklungssystem
- Steuerung über Berechtigungskonzept

2. Integrität

2.1. Weitergabekontrolle

Flowmium gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Bereitstellung der Website und App über verschlüsselte Verbindungen (https)
- Verschlüsselte Verbindung im internen Netz zwischen Application- und Datenbankservern
- E-Mail-Verschlüsselung über TLS und wenn möglich über S/MIME
- Stellung von Hard- und Software für den Home-Office Arbeitsplatz
- Zugang zu Servern (Applikation und Datenbank) nur über VPN möglich
- Ordnungsgemäße Vernichtung von Datenträgern

2.2. Eingabekontrolle

Flowmium gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten nach Benutzer in der Anwendung
- Vergabe von rollenbasierten Berechtigungen in der Anwendung

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Flowmium gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

- Datensicherung mehrmals täglich in einem zweiten Brandabschnitt des Rechenzentrums
- Datensicherung mehrmals täglich in einem georedundanten Rechenzentrum (ab 01.02.2025)
- Backup & Recovery-Konzept
- Regelmäßig Überprüfung der Backups und Tests auf Wiederherstellbarkeit
- Plan für betriebliches Kontinuitätsmanagement und Notfallwiederherstellungsplan
- Dauerhafte Überwachung und Schwachstellenanalyse der Anwendung

3.2. Belastbarkeit

Flowmium gewährleistet die Belastbarkeit der Systeme und Dienste. Dies geschieht durch:

- Einrichtung von Warnregeln zur Erkennung einer erhöhten Serverauslastung
- Regelmäßige Überprüfung der Serverauslastung und Anpassung der Kapazitäten
- Regelmäßige Durchführung von Sicherheits- und Pentests

3.3. Wiederherstellbarkeit

Flowmium gewährleistet die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Dies geschieht durch:

- Backup & Recovery-Konzept
- Regelmäßige Backups der Datenbanken
- Regelmäßige Überprüfung der Backups und Test auf Wiederherstellbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

- Software-Lösungen für Datenschutz-Management im Einsatz
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Datenschutzbeauftragter und Informationssicherheitsbeauftragter bestellt
- Führung des Verzeichnisses der Verarbeitungstätigkeiten
- Regelmäßige Datenschutzaudits
- Unterstützung des Auftraggebers bei Betroffenheitsrechten (Zusammenstellung der Daten für Recht auf Informationen)

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Intrusion Detection System (IDS) im Einsatz
- Intrusion Prevention System (IPS) im Einsatz
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)

- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Es werden datenschutzfreundliche Voreinstellungen (Privacy by default) gewählt.
- Die Anwendung wurde/wird nach dem aktuellen Stand der Technik entwickelt und weiterentwickelt (Privacy by design).

4.4. Auftragskontrolle

Flowmium gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dies geschieht durch:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Laufende Überprüfung der Auftragnehmer und deren Schutzniveaus

Technische und organisatorische Maßnahmen der centron GmbH

centron®

Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Beschreibung der technischen und organisatorischen Maßnahmen

(Art. 32 Abs. 1 lit. d, Art 15 Abs. 1 DS-GVO)

Allgemeine Maßnahmen

- Auf Basis der ISO 27001 wird ein ISMS betrieben
  - Erstzertifizierung 04.04.2020
  - Gültigkeitsdauer 04.07.2026
- TrustedCloud Zertifizierung, 14.06.2014
- Die Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinie ist für alle Mitarbeiter im Zugriff und wird regelmäßig oder bei Bedarf aktualisiert
- Ein Datenschutzbeauftragter ist gestellt und der Geschäftsführung direkt unterstellt
- Ein Risikomanagement ist etabliert und berichtet an die Geschäftsführung
- Eine Notfallplanung und ein Wiederanlaufplan ist etabliert
- Ein Incidentmanagement-System ist etabliert
- Alle Mitarbeiter werden auf die Einhaltung des Datenschutzes und Verschwiegenheit verpflichtet

Trusted Cloud SERVICE 10010

Information Security Management System ISO 27001 Zertifiziert

Testat IT-Grundschutz Basis-Absicherung IGT-0001-2021 centron GmbH

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Vertraulichkeit

Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

- Zugangskontrollsystem
  - Türsicherung im Bürogebäude (elektrische Türöffner mit Zugriffsprotokollierung sowie protokollierte Schlüsselvergabe gemäß Schlüsselmanagement).
  - Zusätzliche biometrische Zugangssicherung zum Rechenzentrum und elektronische Türsicherung zwecks zweistufiger Zutrittskontrolle.
- Einrichtung von Schutzzonen und Festlegung von Zutrittsregeln
- Besucherregelung
  - Protokollierung sämtlicher Besucher
  - Besuche und Lieferanten unterliegen in Abhängigkeit der Schutzzone einer durchgängigen Aufsicht.
- Rundum Videoüberwachung des Gebäude-Außenbereichs mit Sabotageerkennung und Aufzeichnung. Lückenlose Videoüberwachung des Rechenzentrum-Innenbereichs.
- Einbruchmeldeanlage mit Aufschaltung des Sicherheitsdienstes.

Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Erteilung von Berechtigungen nach dem Rollen- und Berechtigungskonzept nach Notwendigkeit
- Festlegung von Berechtigungen durch Leitung der Technik und Geschäftsführung
- Protokollierte Vergabe von Berechtigungen durch die Leitung der Technik
- Arbeitsplatz-PCs sind durch lokale Passwörter der Mitarbeiter geschützt
- Im Intranet werden Passwortrichtlinien durch MS-AD umgesetzt (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Die lokalen Systeme der Mitarbeiter werden regelmäßig bei Erscheinen von Updates aktualisiert
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Vorschaltung einer physikalischen Firewall mit IDS und IPS
- Einsatz von Virenscannern
- Physikalische Trennung von Netzwerken
- Überwachung des Netzwerktraffics

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Passwortvergabe erfolgt ausschließlich durch berechtigtes Personal an vom Auftraggeber benannte Personen
- Die Weisungskommunikation erfolgt auf Seiten des Auftragnehmers über ein ITIL-konformes Ticketsystem
- Die Berechtigung zur Datenverarbeitung personenbezogener Daten werden durch das Active-Directory gesteuert und protokolliert
- Protokollierung der Logins auf den Systemen
- Vernichtung von Datenträgern gemäß Datenträgervernichtungskonzept
- Sofern der Kunde auf seinen Systemen personenbezogene Daten verarbeitet, ist der Kunde primär selbst für die Absicherung der Daten zuständig. Wird diese Zuständigkeit abgetreten, so sind die Sicherungsmechanismen vom Kunden in unregelmäßigen Abständen zu überprüfen und gegebenenfalls zu bemängeln.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Sämtliche Daten können aufgrund der Art ihrer Speicherung getrennt voneinander verarbeitet werden
- Ausschließliche Verwendung von Software, die eine Mandantenfähigkeit bereitstellt
- Trennung der verarbeitenden Systeme
- Trennung der Systeme in Produktiv- und Testumgebung
- Kunden haben gegenseitig keinen Zugriff auf andere Kundensysteme

Integrität

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Eine Weitergabe von personenbezogenen Daten erfolgt nur auf Verlangen von berechtigten Personen oder Institutionen

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

- Sofern eine Übertragung von personenbezogene Daten an berechtigte Personen oder Institutionen stattfindet, erfolgt diese verschlüsselt, auf ausdrücklichen Kundenwunsch auch unverschlüsselt

Datenträger, die personenbezogene Daten enthalten, werden bei einer Entsorgung des Datenträgers mehrfach durch unterschiedliche Löschmethoden bereinigt, anschließend wird der Datenträger zerstört und ordnungsgemäß entsorgt

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Systemaktivitäten durch ein Monitoringsystem
- Teilautomatisierte Auswertung von Logdateien
- Protokollierung aller Arbeiten in ITIL-konformem Ticketsystem
- Neue personenbezogene Daten können nur von berechtigten Personen eingegeben werden

Zugriffe auf das Datenverarbeitungssystem werden (siehe Punkt Zugriffskontrolle) protokolliert.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- RAID (redundante Datenschreibung auf Festplatten)
- Sicherungskopien werden, falls durch Auftraggeber beauftragt, in Form von Backups gemäß Backupkonzept erstellt
- Rhythmus: täglich oder nach Kundenwunsch
- Aufbewahrungszeit: redundant, 1-5 Wochen oder nach Kundenwusch
- Dateiformat: binär, proprietär verschlüsselt
- Aufbewahrungsort ist, je nach Auftrag, dedizierte Storage- oder Serversysteme des Auftraggebers im eigenen oder fremden Rechenzentrum oder globale Storagesysteme des Auftragnehmers, welche wiederum interne Fehlertoleranz aufweisen und mit Zugangskontrollen versehen sind
- Je nach Auftrag durch den Auftraggeber: Konfiguration der Serversysteme mit Hardware-RAID (Spiegelung der Festplatten), redundante Netzteile
- Regelmäßige Prüfung der Backups auf Funktionalität
- Umsetzung von Disaster und Recovery Konzept, Notfallkonzept und Wiederanlaufplan

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Rechenzentrum: Unterbrechungsfreie Stromversorgung (USV), Notstrom-Dieselanlage, redundante Klimaversorgung, Brandfrüherkennungsanlage, regelmäßige Brandbekämpfungsschulungen der Mitarbeiter

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

- Jährliche Überprüfung der Risikoabschätzung für die Verarbeitung personenbezogener Daten
- Jährliche Prüfung der technischen und organisatorischen Maßnahmen auf Angemessenheit und Stand der Technik
- Führen eines zentralen Datenschutzmanagementsystems
- Regelmäßige interne Datenschutz-Audits
- Regelmäßige Schulungen und Sensibilisierungsmaßnahmen zu den Themen Datenschutz und Informationssicherheit

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

- Aufträge durch Kunden die eine Verarbeitung von personenbezogenen Daten verlangen, werden in einem Ticketsystem protokolliert, für das Ticketsystem ist eine Zugriffskontrolle konfiguriert
- Aufträge sind elektronisch nur von verifizierten Kontaktadressen möglich (Email und Fax)
- Aufträge sind ebenfalls per Post in Schriftform nur durch verifizierte Adressen möglich
- Personen, die Aufträge erteilen, müssen vom Vertragspartner für die Erteilung von Aufträgen autorisiert worden sein

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Technische und organisatorische Maßnahmen der IONOS SE

Vereinbarung zur Auftragsverarbeitung - Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art 32 DSGVO

Version 1.0

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.
Festlegung von Sicherheitsbereichen

- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen

Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung der Schnittstellen
- Umsetzung einer Maschine-Maschine-Authentisierung
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery

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

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Resourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess
- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Beachtung von Funktionstrennung und –zuordnung
- Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit STRATO

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Informationssicherheitsmanagement nach ISO 27001
- Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
- Prozess Sicherheitsvorfall-Management
- Durchführung von technischen Überprüfungen

Technische und organisatorische Maßnahmen der inSign GmbH

inSign

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

i.S.d. Art. 32 Abs. 1 DSGVO
Stand 06.11.2023
Version 2.8

inSign

1. Einleitung

Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen stellen wir in der Folge vor.

Gesetzlich geregelt ist die Sicherheit der Verarbeitung in Art. 32 Abs. 1 DSGVO.

2. Organisatorisches

Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. B, 29, 32 Abs. 4 DSGVO und auf ihre Geheimhaltungspflichten gemäß §203 StGB verpflichtet.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden.

3. Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der inSign GmbH betrieben werden:

Kontrollziel	Maßnahmen
3.1. VERTRAULICHKEIT	
3.1.1 Zutrittskontrolle Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	■ Elektronische Zutrittskontrolle zum Firmengebäude und den zentralen Datenverarbeitungsanlagen (Technikräume) ■ Elektronische Protokollierung aller Schließvorgänge (Schlüsselnummer und Zeitstempel) ■ Zentrale Vergabe und Dokumentation der Vergabe der Schließberechtigungen ■ Meldeverpflichtung und Sperre der Zutrittsberechtigung bei Verlust ■ Zugang zu Technikräumen nur für autorisiertes Personal nach ausdrücklicher Genehmigung durch die Geschäftsleitung ■ Aufenthalt von nicht autorisierten Personen in Sicherheitsbereichen nur unter Aufsicht ■ sorgfältige Auswahl des Reinigungspersonals ■ Aktive Netzwerkkomponenten außerhalb der Technikräume befinden sich nur in verschlossenen Sicherheitsschränken
3.1.2. Zugangskontrolle Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	■ Schutz aller Datenverarbeitungsanlagen mindestens durch die Kombination aus Benutzerkennung und Passwort ■ Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten ■ Mindestanforderungen an Passwortkomplexität durch Kennwortrichtlinie ■ Einsatz von Multi-Faktor-Authentifizierung (MFA) ■ Kennwörter müssen geändert werden, wenn der Verdacht auf Kompromittierung des Kennworts (z.B. durch Offenlegung, Hackerangriff, etc.) besteht.

- Falscheingabe des Passworts wird elektronisch protokolliert und führt im Wiederholungsfall zu einer zeitlich begrenzten Deaktivierung des Benutzerkontos
- Verschlüsselte Speicherung von Kennwörtern
- Datenverarbeitungsanlagen sperren die Benutzereingabe, sofern über einen bestimmten Zeitraum keine Interaktion erfolgt
- Netzwerksegmentierung, Verwendung einer Demilitarisierten Zone (DMZ)
- Zugangsbeschränkung für bestimmte IP-Adressbereiche
- Externer Zugang nur über sichere Verbindungen (VPN oder TLS-Verschlüsselung)
- Durchführung regelmäßiger Softwareupdates
- Automatisierte Schwachstellen-Scans
- Protokollierung administrativer Systemzugriffe
- Dokumentation von Konfigurationsänderungen
- Regelmäßige Überprüfung der Zugangsberechtigungen
- Betrieb eines separaten Gast-Netzwerks (Gast-WLAN)
- Einsatz server- und clientseitiger Spamfilter und Antimalwareprogramme (inkl. automatischer Updates)
- Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe).
- Automatisches Netzwerkmonitoring mit Alarmierung.
- Abschaltung/Sperrung nicht benötigter Dienste und Netzwerkports.

3.1.3. Zugriffskontrolle Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der	■ Automatische Prüfung der Zugriffsberechtigung mittels Passwort ■ Ausschließliche Menüsteuerung je nach Berechtigung ■ Aufgaben- und Rollenbasiertes Berechtigungskonzept ■ Trennung von Anwendungs- und Administrationszugängen

Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	■ Externer administrativer Zugriff nur im Ausnahmefall und unter Aufsicht von berechtigtem Personal ■ Durchführung regelmäßiger Softwareupdates ■ Automatisierte Schwachstellen-Scans ■ Protokollierung administrativer Systemzugriffe ■ Dokumentation von Konfigurationsänderungen ■ Personenbezogene Daten, die im Auftrag verarbeitet werden, werden mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik verschlüsselt gespeichert ■ Zugriff auf Backups nur für Administratoren möglich ■ Backups werden mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik verschlüsselt ■ Löschung und Vernichtung von Datenträgern gemäß BSI-Empfehlungen
3.1.4. Trennungsgebot Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	■ Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden voneinander getrennt verarbeitet ■ Trennung von Test- und Produktionsumgebungen ■ Trennung Managementnetz von Produktionsnetz ■ Daten, die im Auftrag verarbeitet werden, werden für jeden Auftraggeber separat auf eigenständigen, getrennten Systemen verarbeitet
3.2. INTEGRITÄT	
3.2.1. Weitergabekontrolle Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	■ Übermittlung personenbezogener Daten mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik (Kryptokonzept) ■ Verschlüsselung von mobilen Endgeräten mit geeigneten Verschlüsselungsverfahren nach dem geltenden Stand der Technik ■ Löschung und Vernichtung von Datenträgern gemäß BSI-Empfehlungen

3.2.2. Eingabekontrolle Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	■ Protokollierung zur nachträglichen Überprüfung der Datenverarbeitung(ssysteme) von: - erfolgreiche und gescheiterte An- und Abmeldevorgänge - Firewall-Protokollierung (TCP/IP) - Protokollierung administrative Tätigkeiten über Ticketsystem ■ Aufbewahrungsfristen für Backups sind festgelegt
3.2.3. Verfügbarkeit und Belastbarkeit Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.	■ Alle Datenverarbeitungsanlagen, auf denen personenbezogene Daten gespeichert werden, befinden sich in ISO/IEC 27001:2013-zertifizierten Rechenzentren ausschließlich in Deutschland. ■ Personenbezogene Daten werden mithilfe automatischer Wiederherstellungs- und Failover-Mechanismen in drei Verfügbarkeitszonen innerhalb eines Rechenzentrums repliziert. ■ Automatisierte Überwachung der gesamten Anlage auf Verfügbarkeit und ordnungsgemäßen Betrieb ■ Protokollierung und Meldung abnormer Ereignisse an zuständige Mitarbeiter ■ Sicherung personenbezogener Daten erfolgt mindestens täglich auf ein eigenständiges, unabhängiges Backupsystem gemäß eines Datensicherungskonzeptes ■ Automatische Funktionsüberwachung der Datensicherung ■ Regelmäßige, stichprobenartige Prüfung der Wiederherstellbarkeit der Daten ■ Antimalwareprogramme sind vorhanden und werden immer auf dem aktuellen Stand gehalten
3.3. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG	
3.3.1. Datenschutz-Management Ein Datenschutzmanagementsystem ist umgesetzt. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen.	

3.3.2. Datenschutzfreundliche Voreinstellungen

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

3.3.3. Auftragskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Alle inSign-Mitarbeiter sind hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.
- Sollte inSign bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden technisch-organisatorische Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO und Art 32 Abs. 1 DSGVO sichergestellt.

  Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses:

  - Vertrag zur Auftragsverarbeitung nach Vorgabe Art. 28 Abs. 3 DSGVO
  - Datenverarbeitung erfolgt ausschließlich innerhalb der EU, bevorzugt in Deutschland
  - Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse
  - Wenn möglich Zertifizierung der Dienstleister nach ISO/IEC 27001:2013
  - Prüfungen und Audits der mit dem Dienstleister vereinbarten Maßnahmen
  - Auf technische Umgebungen von Dienstleistern werden Zugriffsberechtigungen für inSign-Mitarbeiter restriktiv vergeben.
  - Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

inSign

3.4. PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG

Einsatz geeigneter Kryptographieverfahren zur Verschlüsselung von Kommunikationsverbindungen (encryption in transit) und Daten in Ruhe (encryption at rest) an Hand eines Kryptokonzepts.

Zertifikate

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2022**

Zertifikat-Registrier-Nr. **01 153 2300399**

Unternehmen:

Flowmium GmbH
Robert-Bosch-Str. 7
64293 Darmstadt
Deutschland

Geltungsbereich: Entwicklung, Betrieb und Vertrieb von Unternehmenssoftware für den Bereich Personal.

SoA Version 1.1 vom 18.11.2023

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2022 erfüllt sind.

Gültigkeit: Dieses Zertifikat ist gültig vom 18.01.2024 bis 17.01.2027.
Erstzertifizierung 2024

29.01.2024

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Genau. Richtig.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0555-2023

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Prozess Hosting

der centron GmbH

gültig bis: 4. Juli 2026*

Der Prozess Hosting beinhaltet folgende Teilbereiche: Der Betrieb des Rechenzentrums am Standort Hallstadt und der dazu notwendigen Infrastruktur. Unter der Bereitstellung von Rackspace für Kunden. wird die Zurverfügungstellung von Einbauplätzen verstanden. Die centron GmbH stellt das dazu notwendige Rechenzentrum zur Verfügung und betreibt dies. Ebenso wird Strom und ein Netzwerkanschluss bereitgestellt. Seitens der centron GmbH wird die Hardware optional auf Kundenwunsch auf Funktionsfahigkeit überwacht. Bei Defekten werden auf Wunsch des Kunden Hardwarekomponenten ausgetauscht. Weitere IT-Service-Leistungen sind nicht Teil der Bereitstellung von Rackspace. Die Bereitstellung von Servern für Kunden beinhaltet den Betrieb des Rechenzentrums und die Installation, sowie den Betrieb von Serverhardware. Zusätzlich das Monitoring der genannten Serverhardware. Nicht Teil der Bereitstellung von Servern sind die auf den Servern installierten virtuellen Umgebungen, die Betriebssysteme und die installierten Kundenapplikationen. Für diese sind die Kunden vollständig selbst verantwortlich. Der Prozess des Dienstleister-Managements gliedert sich in die Teilbereiche Auswahl, Beauftragung und Überwachung. Zu den relevanten Dienstleistern zählen solche Dienstleister, die Support für die genannten Tätigkeiten und Leistungen der centron GmbH erbringen. Dazu zählen auch insbesondere solche Dienstleister, bei denen Rackspace seitens der centron GmbH angemietet wird. Nicht Teil des Informationsverbundes sind Dienstleister, die Dienstleistungen für die virtuelle Umgebung, Betriebssysteme und Anwendungen der Kunden erbringen. Alle anderen Prozessabläufe der centron GmbH sind nicht Teil des Informationsverbundes.

Der oben aufgeführte Untersuchungsgegenstand wurde von Auditteamleiter Frank-Stefan Stumm, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodik) umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002. Dieses Zertifikat ist keine generelle Empfehlung des Untersuchungsgegenstandes durch das BSI. Eine Gewährleistung für den Untersuchungsgegenstand durch das BSI ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, den 5. Juli 2023
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola
Direktor

* Unter der Bedingung, dass die ab 5. Juli 2023 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn · Postfach 20 03 63, D-53113 Bonn
Tel.: +49 (0)228 9582-0 · Fax: +49 (0)228 9582-5477 · Infoline: +49 (0)228 9582-111 · Internet: www.bsi.bund.de

TÜV NORD

ZERTIFIKAT

für das Managementsystem nach

ISO/IEC 27001 : 2013

(Einschließlich Cor 1:2014 und Cor 2:2015)

Die Zertifizierungsstelle TÜV NORD CERT GmbH bestätigt hiermit als Ergebnis der Auditierung, Bewertung und Zertifizierungsentscheidung gemäß ISO/IEC 27006:2015/Amd.1:2020, dass die Organisation

IONOS Holding SE
Elgendorfer Straße 57
56410 Montabaur
Deutschland

IONOS

mit den Standorten gemäß Anlage

ein Managementsystem konform zu den Anforderungen der ISO/IEC 27001 : 2013 betreibt und innerhalb der Laufzeit des Zertifikats von 3 Jahren auf Konformität überwacht wird.

Geltungsbereich

Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen sowie Managed Internet Services in den Rechenzentren der IONOS Gruppe sowie der zugehörige Kundenservice

Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0

Zertifikat-Registrier-Nr. 44 121 160247
Auditbericht-Nr. 3531 7732

Gültig von 2022-04-19
Gültig bis 2025-04-18
Erstzertifizierung 2016

Zertifizierungsstelle
der TÜV NORD CERT GmbH

Essen, 2022-04-19

Die Gültigkeit kann unter https://www.tuev-nord.de/de/unternehmen/zertifizierung/zertifikatsdatenbank verifiziert werden.

TÜV NORD CERT GmbH | Am TÜV 1 | 45307 Essen | www.tuev-nord-cert.de

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

DAkkS Deutsche Akkreditierungsstelle D-ZM-12007-01-00

TÜV NORD

ANLAGE

zum Zertifikat Registrier-Nr. 44 121 160247
ISO/IEC 27001 : 2013
(Einschließlich Cor 1:2014 und Cor 2:2015)

IONOS Holding SE
Elgendorfer Straße 57
56410 Montabaur
Deutschland

IONOS

Zertifikats-Reg.-Nr.	Standort	Geltungsbereich
44 121 160247-001	IONOS Holding SE c/o IONOS Inc. 701 Lee Road Chesterbrook PA 19087 USA	Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der IONOS sowie der zugehörige Kundenservice Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0
44 121 160247-002	IONOS Holding SE c/o Fasthosts Internet Limited Discovery House, 154 Southgate Street Gloucester GL1 2E Vereinigtes Königreich	Betrieb von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der Fasthosts Internet Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0
44 121 160247-003	IONOS Holding SE c/o Arsys Internet S.L.U. C/ Madre de Dios 21 26006 Logroño (La Rioja) Spanien	Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der Arsys Internet Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de

Seite 1 von 2

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
DAkkS Deutsche Akkreditierungsstelle D-ZM-12007-01-00

TÜV NORD

ANLAGE

zum Zertifikat Registrier-Nr. 44 121 160247
ISO/IEC 27001 : 2013
(Einschließlich Cor 1:2014 und Cor 2:2015)

Zertifikats-Reg.-Nr.	Standort	Geltungsbereich
44 121 160247-012	IONOS Holding SE c/o IONOS SE Elgendorfer Straße 57 56410 Montabaur Deutschland	Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der IONOS sowie der zugehörige Kundenservice Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0
44 121 160247-013	IONOS Holding SE c/o Strato AG Otto-Ostrowski Straße 7 10249 Berlin Deutschland	Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der Strato sowie der zugehörige Kundenservice Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0
44 121 160247-014	IONOS Holding SE c/o Cronon GmbH Otto-Ostrowski Straße 7 10249 Berlin Deutschland	Betrieb und Entwicklung von Managed Internet Services, Infrastruktur und Plattformen Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0
44 121 160247-015	IONOS Holding SE c/o Strato Customer Service GmbH Otto-Ostrowski Straße 7 10249 Berlin Deutschland	Kundenservice für Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der Strato Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 17.02.2022, Version 4.0

- Ende der Auflistung -

Zertifizierungsstelle
der TÜV NORD CERT GmbH

Essen, 2022-04-19

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de

Seite 2 von 2

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
DAkkS Deutsche Akkreditierungsstelle D-ZM-12007-01-00

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0543-2022

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Bereitstellung und Betrieb von IONOS Cloud Services in Deutschland

der IONOS SE

gültig bis: 13. September 2025*

Der Untersuchungsgegenstand umfasst die Kern- und Unterstützungsprozesse sowie Anwendungen, IT-Systeme und Rechenzentrumsstandorte der IONOS, welche notwendig sind, um IONOS Cloud Services in Deutschland bereitzustellen und zu betreiben. Der betrachtete Informationsverbund besteht aus:

- ISMS der IONOS Gruppe und Infrastruktur für die IONOS Cloud Services in Deutschland,
- IONOS Cloud Compute Engine und S3 Object Storage inkl. Provisionierung,
- IONOS Cloud Backup sowie
- IONOS Cloud Managed Services.

Der oben aufgeführte Untersuchungsgegenstand wurde von Peter Herrmann, zertifizierter Auditor für ISO 27001-Audits auf der Basis von ITGrundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002. Dieses Zertifikat ist keine generelle Empfehlung des Untersuchungsgegenstandes durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Untersuchungsgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, 14. September 2022

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Sandro Amendola
Abteilungspräsident

*Unter der Bedingung, dass die ab 14. September 2022 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 9582-111

swiss safety center

Zertifikat

swiss safety center ISO/IEC 27001 certified system

Die Zertifizierungsstelle von Swiss Safety Center AG
bescheinigt, dass die Firma

BSI Business Systems Integration AG
Täfernweg 1
CH-5405 Baden

BSI Business Systems Integration
Deutschland GmbH
Rheinstrasse 97
D-64295 Darmstadt

bsi

inSign GmbH
Am Bäckeranger 2
D-85417 Marzling

mit den Standorten gemäss Anhang

für den Geltungsbereich

Entwicklung, Betrieb und Support von Cloud-Dienstleistungen (SaaS)

ein **Informationssicherheitsmanagementsystem (ISMS)**
erfolgreich anwendet nach

ISO/IEC 27001:2013

Erklärung zur Anwendbarkeit:	**08.08.2022 (v.84)**
Registriernummer:	**22-165-714**
Erstzertifizierung:	**04.10.2022**
Gültig ab:	**04.04.2024**
Gültig bis:	**03.10.2025**

Heinrich A. Bieler
Leiter der Zertifizierungsstelle

Wallisellen, 08.04.2024

Swiss Safety Center AG, Certifications
Richtistrasse 15, CH-8304 Wallisellen
Ein Unternehmen der SVTI-Gruppe, Mitglied des TÜV-Verbands.

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

SWISS ACCREDITATION sas.admin.ch SCES m 0013

Datenschutz Pöllinger GmbH
Datenschutz und Informationssicherheit

Prüfbericht

Flowmium GmbH
Erich-Kästner-Str. 55
63322 Rödermark

Die Prüfung des Unternehmens sowie der Software „Zeugnisgenerator“ in Bezug auf die Verarbeitung von personenbezogenen Daten im Auftrag ergibt, dass die Flowmium GmbH datenschutzrechtlich gut aufgestellt ist und im Laufe des Jahres 2021 zahlreiche datenschutzrechtliche Prozesse bezüglich der Anforderungen der EU Datenschutz-Grundverordnung (DS-GVO) weiterentwickelt und optimiert wurden.
Das Datenschutzmanagementsystem der Flowmium GmbH wurde durch ein eigeninitiativ gewünschtes Audit anhand von verschieden Checklisten, welche IT-Sicherheit, Backup und Datenschutz betreffen, durchgeführt. Hierbei wurde festgestellt, dass die Flowmium GmbH bereits sehr gut aufgestellt ist. Anhand von einer Defizitliste wurde der Flowmium GmbH eine Handlungsempfehlung übergeben, damit das Datenschutzmanagement für die Zukunft noch weiter ausgebaut und kontinuierlich optimiert werden kann.

Die Software „Zeugnisgenerator“ erfüllt die Anforderungen nach Privacy by Design und Privacy by Default nach Artikel 25 DS-GVO. Der Kunde, als verantwortliche Stelle, kann dabei entsprechende Maßnahmen treffen und ist für die Umsetzung der entsprechenden Einstellungen innerhalb der Software selbst verantwortlich.

Weiterhin werden die Grundsätze der Verarbeitung von personenbezogenen Daten, insbesondere Transparenz, Treu und Glauben, Zweckbindung und Datenminimierung entsprechend beachtet. Es werden grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet.
Der Kunde, als Verantwortlicher, hat die Rechtmäßigkeit der Datenverarbeitung selbst sicherzustellen und kann den Umfang der Verarbeitung entsprechend über die Software selbst steuern. Zudem hat der Kunde die Möglichkeit, den Zugang anhand eines Berechtigungskonzepts selbst zu steuern. Entsprechende datenschutzrechtliche Voreinstellungen sowie zusätzliche technische und organisatorische Maßnahmen stellen dabei sicher, dass Unbefugte keinen Zugriff auf die Software erhalten.

Ferner hat die Flowmium GmbH ein umfangreiches Datenschutz- und IT-Sicherheitskonzept aufgestellt und daraus entsprechende technische und organisatorische Maßnahmen abgeleitet, welchen den Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO genügen.

Dresdner Straße 38
92318 Neumarkt
kontakt@datenschutz-poellinger.de
09181/270 577 0
www.datenschutz-poellinger.de

Zudem sind bereits in der Vergangenheit entsprechende Prozesse implementiert worden, um die kontinuierliche Verbesserung der Prozesse und Prüfung und Weiterentwicklung dieser Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten dem Umfang der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sicherzustellen.

Die Mitarbeiter der Flowmium GmbH wurden durch eine Online-Schulung „Datenschutz und Informationssicherheit im Unternehmen“ im September 2021 geschult. Nach der Online-Schulung fand eine Prüfung zur Erlangung des Zertifikates statt. Alle Mitarbeiter haben die Prüfung mit Erfolg bestanden. Ferner wurden alle Mitarbeiter auf Datenschutz und Vertraulichkeit verpflichtet.

Zusammenfassend kann festgehalten werden, dass die Software in ihrer Konzeption und Umsetzung die Anforderungen an Entwicklung und Betrieb von Software im Sinne der EU DS-GVO umfassend erfüllt. Gleiches gilt für die Organisation und das Datenschutzmanagement in Bezug auf die Auftragsverarbeitung für die Kunden der Flowmium GmbH.

Gisela Pöllinger

Neumarkt, den 24.09.2021

Gisela Pöllinger
Auditorin für Datenschutz & Informationssicherheit

Datenschutz Pöllinger GmbH
Datenschutz und Informationssicherheit

DESAG
Sachverständiger
Gisela Pöllinger
DS/210501

Dresdner Straße 38
92318 Neumarkt
kontakt@datenschutz-poellinger.de
09181/270 577 0
www.datenschutz-poellinger.de

ZERTIFIKAT

Penetrationstest

Für die **Flowmium GmbH** aus Darmstadt
führte die binsec GmbH vom
20. Januar 2025 bis **23. Januar 2025** einen Penetrationstest durch.

Prüfgegenstand

Die Webanwendung der Flowmium GmbH zur Erstellung von Arbeitszeugnissen wurde einem Penetrationstest unterzogen. Für die Untersuchung der Webanwendung wurde eine Testumgebung zur Verfügung gestellt. Der Penetrationstest wurde als externer Grey-Box-Test durchgeführt, ohne aggressive Angriffstechniken wie DDoS-Attacken zu verwenden. Die Untersuchungsmethode orientierte sich am OWASP Testing Guide und an den OWASP TOP 10.

Prüfergebnis

Im Rahmen des Penetrationstests wurden Schwachstellen mit Handlungsbedarf identifiziert, welche bis zum 27. Januar 2025 erfolgreich behoben wurden. Dies wurde von der binsec GmbH in einer Nachprüfung verifiziert.

Erläuterung

In einem Penetrationstest werden IT-Systeme oder IT-Anwendungen basierend auf einer strukturierten Vorgehensweise unter Verwendung von Hacking-Tools und -Techniken auf Schwachstellen hin analysiert. Die Ergebnisse des Penetrationstests sind immer eine Momentaufnahme der IT-Sicherheit. Je länger dieser zurückliegt und je mehr Änderungen vorgenommen werden, desto geringer wird die Aussagekraft der Ergebnisse. Ein Penetrationstest sollte somit jährlich oder nach signifikanten Änderungen wiederholt werden. Mehr Informationen zu den Penetrationstests der binsec GmbH finden Sie im Web unter `https://binsec.com/pentest/`.

Dominik Sauer, ppa
Head of Penetration Testing

PENTESTED BY BINSEC 2025