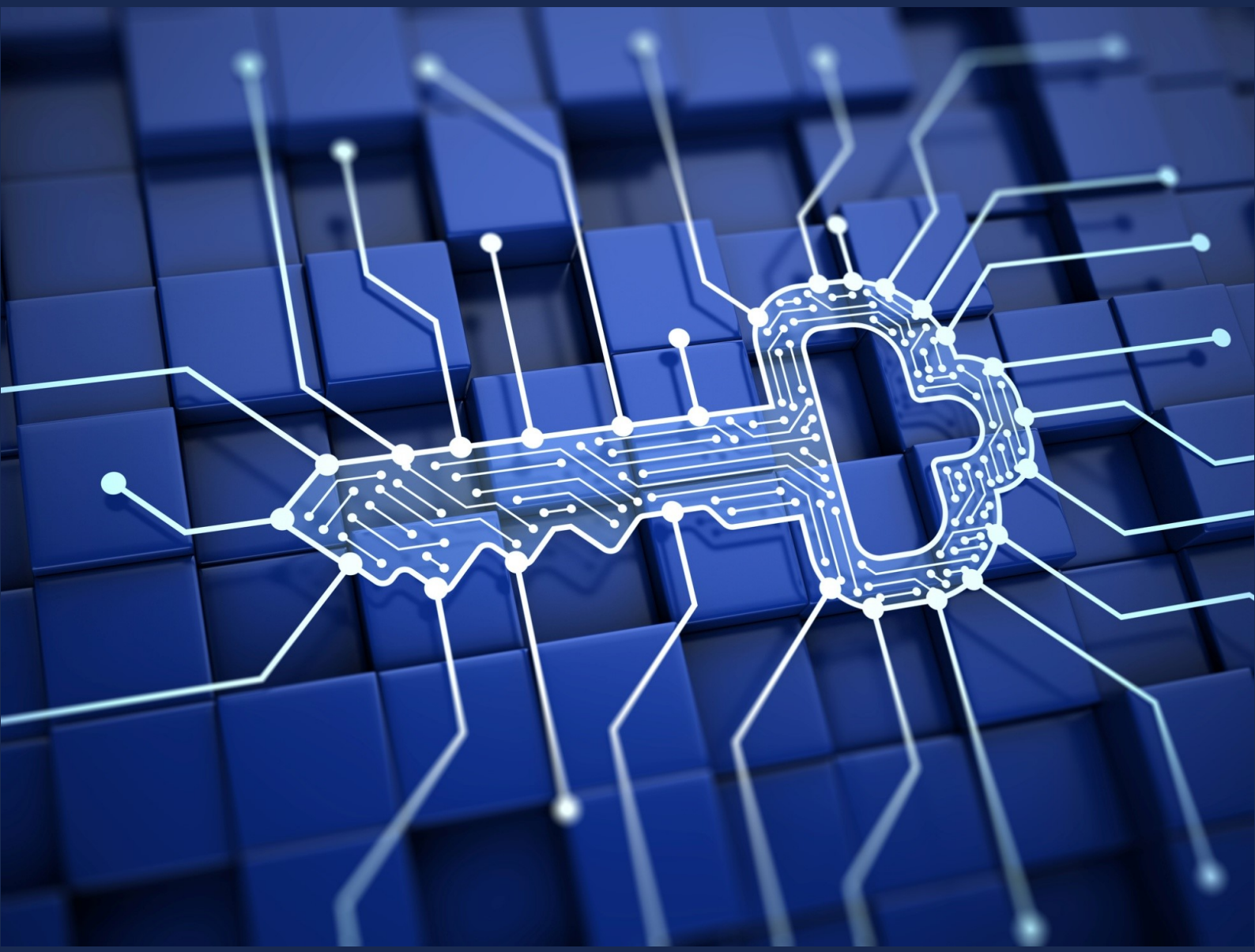
Dokumentation

Technische und organisatorische Maßnahmen (TOM)



Neuland IT Solutions GmbH & Co. KG
Auricher Straße 162
26624 Südbrookmerland

Inhaltsverzeichnis

1. Verantwortlicher

Neuland IT Solutions GmbH & Co. KG
Auricher Straße 162
26624 Südbrookmerland

Gesetzlicher Vertreter/Geschäftsführer/Inhaber: Keven Böhm, Hendrik Neuland
Tel.: 049318206312
E-Mail: kb@neuland-it.de
Internet: https://neuland-it.de

Zuständige Aufsichtsbehörde:
Der Landesbeauftragte für den Datenschutz Niedersachsen, Prinzenstraße 5, 30159 Hannover, Telefon: 05 11/120-45 00, E-Mail: poststelle@lfd.niedersachsen.de, Homepage: https://www.lfd.niedersachsen.de

2. Externer Datenschutzbeauftragter

DATENDO GmbH
Hohenzollernring 55
50672 Köln
Tel. 0800 5577733
E-Mail: dsgvo@datendo.de
Internet: www.datendo.de

3. Gültigkeit

Die technischen und organisatorischen Maßnahmen wurden zuletzt geändert am: 22.11.2025

Diese Dokumentation der technischen und organisatorischen Maßnahmen ist gültig bis einschließlich zum: 22.11.2026

Mit Ablauf der laufenden Gültigkeitsperiode findet eine Überprüfung und gegebenenfalls eine Aktualisierung der derzeit umgesetzten und dokumentierten Maßnahmen statt.

4. Technische und organisatorische Maßnahmen (TOM)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, Art. 32 Absatz 1 DSGVO.

Vor diesem Hintergrund sind in unserem Unternehmen die folgenden technischen und organisatorischen Maßnahmen im Sinne des Artikels 32 DSGVO zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten umgesetzt:

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

Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.

Umgesetzte Maßnahmen:

- Verwendung einer Alarmanlage
- Datenschutzkonforme Videoüberwachung der Eingänge
- Abschließbare Türen
- Manuelle Schließsysteme
- Sicherheitsschlösser
- Zugang per Klingel mit Kameraanlage
- Türen mit Knauf an der Außenseite
- Code, Transponder- oder Chipkarten für den Zutritt
- Server befindet sich in einem verschlossenen Raum/Serverschrank
- Elektrische Türöffner
- Sorgfältige Auswahl von Wachschutz und Reinigungsdiensten
- Dienstanweisung zum Verschließen der Räume
- Besucheranmeldung, Besucherabmeldung (Besuchererfassung/Protokollierung)
- Besucher können das Gebäude nur betreten, wenn sie von einem der Beschäftigten in Empfang genommen und begleitet werden
- Ständige Anwesenheit von Personal während der Besuchszeiten

Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Umgesetzte Maßnahmen:

- Logins erfolgen mit Benutzername/Passwort
- Logins erfolgen mit biometrischen Daten
- Logins erfolgen mit Softwarezertifikat
- Ein aktueller Spamfilter findet Verwendung
- Ein aktueller Virenscanner findet Verwendung
- Eine aktuelle Firewall findet Verwendung
- Es werden aktuelle Softwareversionen verwendet
- E-Mails werden verschlüsselt
- Eine automatische Desktopsperre kommt bei Inaktivität zur Anwendung
- Der Zugriff auf Endgeräte ist verschlüsselt (Passwort, Fingerabdruck, Gesichtserkennung)
- Es findet eine verschlüsselte Datenübertragung (https/TLS) statt.
- Im Unternehmen besteht eine Unternehmensrichtlinie zum Datenschutz
- Es besteht eine Richtlinie zum Einsatz von USB-Sticks
- Es besteht eine Richtlinie zum verpflichtenden Einsatz einer Bildschirmsperre
- Es besteht eine Clean-Desk Vorgabe
- Monitore sind stets sichtgeschützt aufgestellt
- Im Unternehmen kommen Benutzerprofile zum Einsatz
- Es besteht ein Verfahren zur Vergabe von Lese- und Schreibrechten (Benutzerverwaltung)

Zugriffskontrolle

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

Umgesetzte Maßnahmen:

- Datenträger werden verschlüsselt
- Nicht mehr benötigte Datenträger werden physisch gelöscht
- Zugriffe auf Anwendungen und Prozesse werden protokolliert
- Verwendung von Aktenvernichtern
- Verwendung von Datenträgervernichtern
- Die Anzahl der Administrationen, mit vollem Zugriff, wird minimal gehalten
- Benutzerrechte werden durch Administratoren anhand eines Rollen- und Berechtigungskonzepts vergeben
- Die Löschung und Vernichtung von Daten wird protokolliert
- Für die Nutzung von PCs durch mehrere Beschäftigte bestehen individuelle Benutzerkonten
- Es besteht eine Richtlinie zur Generierung sicherer Passwörter

Trennungskontrolle

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

Umgesetzte Maßnahmen:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung der Systeme, Datenbanken und Datenträger
- Trennung anhand der Ordnerstrukturen einer Festplatte
- Steuerung der Verarbeitung anhand eines Berechtigungskonzepts
- Festlegung von Datenbankzugriffsrechten
- Steuerung der Verarbeitung durch jeweils angepasste Datenbankzugriffsrechte

Pseudonymisierung

Maßnahmen, die gewährleisten, dass die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden und auch nicht zugewiesen werden können.

Umgesetzte Maßnahmen:

- Wir haben Pseudonymisierung als technische Maßnahme zur Verbesserung des Schutzes von personenbezogenen Daten geprüft. Aktuell können wir Maßnahmen zur Pseudonymisierung jedoch nicht implementieren.

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

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 werden kann, an welche Stellen eine Übermittlung personenbezogener Daten zur Datenübertragung vorgesehen ist.

Umgesetzte Maßnahmen:

- E-Mails werden verschlüsselt
- Datenträger werden verschlüsselt
- Verwendung einer elektronischen Signatur für E-Mails
- Einsatz von VPN
- Nutzung von Signaturverfahren
- Protokollierung von Zugriffen und Abrufen
- Bereitstellung über verschlüsselte Verbindungen (zB SFTP oder https)
- Es werden sichere verschlossene Transportbehältnisse verwendet
- Es wird zuverlässiges Transportpersonal eingesetzt
- Persönliche Übergabe, die protokolliert wird
- Die Empfänger von Daten werden dokumentiert und kontrolliert

Eingabekontrolle

Maßnahmen, die es erlauben, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind und ob diese den Ursprungsdaten entsprechen.

Umgesetzte Maßnahmen:

- Die Eingabe, Veränderung und Löschung von Daten werden technisch protokolliert
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Zugriffsberechtigungen
- Formulare, von denen Daten in automatisierte Verarbeitungen übertragen wurden, werden aufbewahrt

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

Verfügbarkeitskontrolle und Wiederherstellbarkeit

Maßnahmen zur Wahrung der Verfügbarkeit und Belastbarkeit sollen sicherstellen, dass verarbeitete personenbezogene Daten auch nach einem Zwischenfall weiterhin zur Verfügung stehen, um den Betrieb wieder aufzunehmen. Maßnahmen zur Wiederherstellbarkeit gewährleisten die zeitnahe Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust.

Umgesetzte Maßnahmen:

- Brandschutzeinrichtungen (z.B. Feuer- und Rauchmeldeanlage)
- Feuerlöscher im Betrieb
- Feuerlöscher im Serverraum
- Überspannungsschutz
- Serverraum ist klimatisiert
- System zur Serverraumüberwachung (zB Temperatur und Feuchtigkeit)
- Rauchverbot im Betrieb
- Unterbrechungsfreie Stromversorgung (USV)
- Datensicherungskonzept vorhanden
- Backup-Konzept
- Regelmäßige Datensicherungen (Backups)
- Speicherung von Backups an einem externen Ort
- Spiegeln von Festplatten (Raid-System, Spiegelung)
- Notfallplan/Wiederanlaufplan
- Tests zur Wiederherstellung von Datenbeständen aus Backups

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, also Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Umgesetzte Maßnahmen:

- Es werden nicht mehr Daten erhoben, als dies für den Zweck erforderlich ist
- Beschränkung der Speicherdauer anhand einer technischen Voreinstellung/Programmierung
- Beschränkung der Zugänglichkeit durch eine technische Voreinstellung

Auftragskontrolle

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

Umgesetzte Maßnahmen:

- Sorgfältige Auswahl von Auftragsverarbeitern
- Abschluss eines Auftragsverarbeitungsvertrags
- Vereinbarung von Kontrollrechten
- Mitarbeiter werden zur Vertraulichkeit verpflichtet

Datenschutz-Management

Die zum Datenschutz-Management veranlassten weiteren Maßnahmen sind dem Datenschutz-Management-Handbuch unseres Unternehmens zu entnehmen.