Angaben zum Dokument

Titel des Dokuments	Datenschutz-Maßnahmen
Eigentümer	CEO
Status	ABGENOMMEN
Klassifizierung	Vertraulich – Extern
Version	2.0.EU
Datum	19. September 2023
Nächste Überprüfung	10. Januar 2024

Version	Änderung	Initialen	Datum
1.0	Für neue Organisation erstellt	SXF	25. Aug. 2023
1.1	Erste Bearbeitungen nach Peer Review	CS	8. Sept. 2023
2.0	Genehmigung „Vertraulich Extern“ (CEA)	JY	19. Sept. 2023

Abnahmen

Version	Rolle	Initialen	Datum
1.0	Nur Entwürfe mit Klassifizierung		
2.0	CEO	JY	19. Sept. 2023

EINLEITUNG

Dieses Dokument beschreibt die konkreten Datenschutzmaßnahmen, die von ForeNova im Einklang mit dem deutschen Sicherheits- und Compliance-Standard TOM (Technische und Organisatorische Maßnahmen) umgesetzt werden. Die Maßnahmen werden sowohl aus organisatorischer als auch aus technischer Sicht beschrieben, um eine umfassende Datensicherheit zu gewährleisten.

2. ORGANISATORISCHE SICHERHEITSMASSNAHMEN

2.1 Datenschutzorganisation

ForeNova misst dem Datenschutz große Bedeutung bei, indem sie:

2.1.1 eine Data-Governance-Rahmenordnung einrichtet und pflegt, mit der Aufgaben, Zuständigkeiten und Verantwortlichkeiten für den Datenschutz festlegt werden,

2.1.2 einen Datenschutzbeauftragten bestellt, der für die Überwachung und Verwaltung von Datenschutzangelegenheiten zuständig ist,

2.1.3 ein Datenschutz-Team aufstellt, welches zuständig ist für das tägliche Datenschutz-Management und die Reaktion auf Vorfälle.

2.2 Risikomanagement

ForeNova hat einen Risikomanagement-Mechanismus eingerichtet und nutzt seine eigenen Risikomanagement-Dienste in vollem Umfang für die Steuerung von Datenschutzrisiken. Zum Beispiel:

2.2.1 Durchführung regelmäßiger Risikobewertungen zur Ermittlung potenzieller Schwachstellen und Bedrohungen des Datenschutzes und Entwicklung und Umsetzung von Strategien zur Risikominderung auf der Grundlage der ermittelten Risiken,

2.2.2 Einführung von Verfahren für die Reaktion auf und den Umgang mit Vorfällen für eine wirksame Behandlung von Datenschutzverletzungen,

2.2.3 Durchführung von Angriffs- und Abwehrübungen zur proaktiven Ermittlung potenzieller Datenschutzrisiken Ergreifen von geeigneten Maßnahmen zur Bewältigung dieser Risiken.

2.3 Mitarbeitersicherheit

2.3.1 Alle ForeNova-Mitarbeiter werden vor ihrem Eintritt in das Unternehmen einer Hintergrundüberprüfung unterzogen, um sicherzustellen, dass ihr Hintergrund den gesetzlichen Anforderungen entspricht.

2.3.2 Zur Gewährleistung, dass alle neuen Mitarbeiter sich ihrer Verpflichtung zur Wahrung des Datengeheimnisses bewusst sind, wird eine Geheimhaltungsvereinbarung (NDA) unterzeichnet.

2.3.3 ForeNova führt regelmäßig Datenschutz- und Sicherheitsschulungen für ihre Mitarbeiter durch, um das Bewusstsein für den Datenschutz zu schärfen und die Einhaltung der Datenschutzrichtlinien zu fördern.

2.3.4 Ausscheidenden Mitarbeitern werden die Systemberechtigungen umgehend entzogen und sie werden aufgefordert, alle unternehmenseigenen Gegenstände zurückzugeben.

2.4 Physische Sicherheit

ForeNova hat sich für einen Rechenzentrumsdienstleister entschieden, dem weltweit

Vertrauen entgegengebracht wird und der mehrere Sicherheitszertifizierungen erlangt und mehrere Sicherheitsmaßnahmen implementiert hat, um die physische Sicherheit seines Rechenzentrums zu gewährleisten.
Normenkonformität Das Rechenzentrum erfüllt die physischen Sicherheitskontrollen in Übereinstimmung mit Normen und Vorschriften wie ISO27001, SOC 2 Typ II, EU-Verhaltenskodex und vielen weiteren Qualitäts-, IKT- und Cybersicherheitsstandards.

Zugangskontrolle Das Rechenzentrum setzt rund um die Uhr Sicherheitspersonal vor Ort, Videoüberwachung, biometrische Authentifizierungssysteme und sichere Umzäunungen ein, um sicherzustellen, dass nur befugtes Personal Zugang zu den Einrichtungen des Rechenzentrums hat.
Zuverlässigkeit und Ausfallsicherheit Das Rechenzentrum gewährleistet einen unterbrechungsfreien Betrieb und Datenschutz durch redundante Stromversorgungssysteme, Geräte, Ersatzgeneratoren und mehrere Netzwerkverbindungen.

2.5 Datenklassifizierung

ForeNova setzt Richtlinien zur Datenklassifizierung und Kennzeichnung ein, um einen angemessenen Umgang mit und Schutz von sensiblen Daten zu gewährleisten.

2.6 Compliance Management

ForeNova hat eine Datenschutz-Compliance-Gruppe bestehend aus Rechts- und Sicherheitsfachkräften sowie Vertretern der Geschäftsabteilungen zusammengestellt. Diese Gruppe hat die Aufgabe, die einschlägigen datenschutzrechtlichen Vorschriften umgehend zu ermitteln und zu bewerten.

3. TECHNISCHE SICHERHEITSMASSNAHMEN

3.1 Zugriffskontrolle

ForeNova implementiert einen robusten Zugriffskontrollmechanismus, um sicherzustellen, dass nur autorisiertes Personal auf Daten zugreifen und diese verarbeiten kann. Dieser Zugriffskontrollmechanismus umfasst:
3.1.1 die Implementierung eines Zugriffssteuerungsverfahrens, mit dem Benutzerrechte nach dem Prinzip der geringstmöglichen Berechtigung und Kenntnis nur wenn notwendig zugeordnet werden,
3.1.2 die Erzwingung starker Passwortrichtlinien und die Förderung der Multi-Faktor-Authentifizierung für alle Benutzerkonten,
3.1.3 die Führung detaillierter Protokolle und Prüfpfade über die Benutzeraktivitäten innerhalb des Systems. Dies ermöglicht die Überwachung und Identifizierung unbefugter Zugriffsversuchen oder verdächtigen Verhaltens,
3.1.4 die regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte der Nutzer und den sofortigen Entzug des Zugriffs bei Bedarf.

3.2 Netzwerksicherheit

ForeNova setzt hochentwickelte Technologien und Lösungen ein, um das Risiko von Datenschutzverletzungen durch Netzwerksicherheit zu verhindern. Diese umfassen mindestens:
3.2.1 den Einsatz hochentwickelter Firewalls der nächsten Generation sowie von Intrusion

Detection und Prevention Systemen, um unbefugte Zugriffe und Cyberangriffe in Echtzeit zu erkennen und zu blockieren,
3.2.2 die Netzwerksegmentierung zum Schutz vor unbefugtem Zugriff und externen Bedrohungen,
3.2.3 den Einsatz einer Zero-Trust-Lösung, die ein Minimum an Diensten und Ports zum Internet hin öffnet und die Gefährdung des Netzwerks minimiert,
3.2.4 das regelmäßige Aktualisieren und Patchen von Sicherheitsgeräten, -anwendungen und -komponenten, um bekannte Schwachstellen zu beseitigen.

3.3 Sicherheitsmaßnahmen

3.3.1 ForeNova setzt eine eigene Sicherheitslösung mit dem Namen „Component + Platform + Service“ für die Erkennung und Reaktion ein.

3.3.2 ForeNova hat eigene Sicherheitskomponenten wie NovaCommand und NovaGuard eingesetzt, die sich in unsere Sicherheitsplattform NovaMDR integrieren und so eine rechtzeitige Erkennung und Identifizierung möglicher Bedrohungen und das Ergreifen geeigneter Maßnahmen in Reaktion darauf ermöglichen.
3.3.3 Das eigene professionelle Sicherheitsexpertenteam von ForeNova betreibt rund um die Uhr ein Monitoring des sicherheitsrelevanten Betriebs und die Reaktion auf Vorfälle.

3.4 Data Lifecycle Management

ForeNova ergreift Sicherheits- und Compliance-Maßnahmen zum Umgang mit Daten über deren gesamten Lebenszyklus hinweg, einschließlich:

3.4.1 Datenerfassung

Die Datenerfassung erfolgt in Übereinstimmung mit den rechtlichen Vorschriften, indem nur die für den Geschäftsbetrieb notwendigen personenbezogenen Daten erfasst werden und das ausdrückliche Einverständnis des Kunden eingeholt wird.

3.4.2 Datenübermittlung

Zur Gewährleistung der Sicherheit der Datenübertragung kommen das sichere Übertragungsprotokoll TCP auf der Netzwerkschicht, TLS auf der Sitzungsschicht und HTTPS auf der Anwendungsschicht zum Einsatz.

3.4.3 Datenverwendung

Die Nutzung von Daten ist eingeschränkt; nur befugtes Personal hat für geschäftliche Zwecke Zugriff auf sensible Daten, und die Darstellung sensibler Daten erfolgt in anonymisierter Form.
Alle Zugriffs- und Betriebsprotokolle werden aufgezeichnet und überprüft.
Einsatz der UEM-Sandbox-Technologie zur Sicherstellung, dass der Zugriff auf die Daten der Produktionsumgebung innerhalb der Sandbox erfolgt und so verhindert wird, dass Daten auf persönlichen Endgeräten gespeichert werden und das Risiko von Datenlecks verringert wird.

3.4.4 Datenspeicherung

Zum Schutz der gespeicherten personenbezogenen Daten wird ein starker Verschlüsselungsalgorithmus (AES-256) verwendet, und für den Notfall werden Kopien aller wichtigen Daten aufbewahrt.
Implementierung von Schlüsselverwaltungspraktiken zum Schutz der Schlüssel für die

Verschlüsselung.

3.4.5 Datenextraktion

Die Extraktion aller Produktionsdaten wird durch ein Genehmigungsverfahren kontrolliert, um sicherzustellen, dass die Datenextraktion den Geschäftsanforderungen entspricht.
Alle Genehmigungsunterlagen werden aufbewahrt, um sicherzustellen, dass die extrahierten Daten überprüfbar und nachvollziehbar sind.

3.4.6 Datenaufbewahrung und -beseitigung

Festlegung und Erzwingung von Richtlinien zur Datenaufbewahrung, die im Einklang mit den gesetzlichen und behördlichen Vorschriften stehen.
Vor dem Auslaufen des Dienstes wird ForeNova den Kunden benachrichtigen und mit ihm über die Art der Datenverarbeitung nach dem Auslaufen des Dienstes verhandeln.
Implementierung sicherer Verfahren zur Datenbeseitigung auf der Grundlage der Anforderungen des Kunden, einschließlich der Verwendung von Datenvernichtungsmethoden wie Verschlüsselung oder physische Vernichtung.

3.5 Schwachstellen-Management

3.5.1 ForeNova führt regelmäßige Schwachstellen-Scans durch und bewertet die Sicherheitslage von Systemen, Anwendungen und Infrastruktur.
3.5.2 Festgestellte Schwachstellen wird ForeNova umgehend durch Patches oder andere Maßnahmen zur Schadensbegrenzung beheben.

3.5.3 ForeNova führt Penetrationstests durch, um potenzielle Sicherheitsschwächen zu ermitteln und eine kontinuierliche Verbesserung der Sicherheitsmaßnahmen zu gewährleisten.
3.5.4 ForeNova verfolgt einen Prozess für das Management von Schwachstellen und setzt eine Schwachstellen-Management-Plattform ein, um das Auffinden, die Disposition, Validierung und Schließung von Schwachstellen über den gesamten Prozesses hinweg zu verfolgen und zu steuern.

3.6 Vorfall-Reaktions-Management

3.6.1 ForeNova hat einen Prozess für die Reaktion auf Vorfälle eingeführt, der eine definierte Reaktionsorganisation, Rollen, Personal und Verantwortlichkeiten für den Umgang mit Vorfällen umfasst.
3.6.2 Vorfälle werden in verschiedene Stufen und unterschiedliche Arten der Bearbeitung und Meldung eingeteilt. ForeNova organisiert regelmäßig Treffen der zuständigen Mitarbeiter, um über den Reaktionsprozess auf Vorfälle zu sprechen und ihn bekannt zu machen, so dass jeder mit seinen Aufgaben vertraut ist.
3.6.3 Ausarbeitung einer Notfallplanung und Durchführung regelmäßiger Übungen zur Reaktion auf Vorfälle sowie
Simulationen zur Überprüfung der Wirksamkeit des Plans.
3.6.4 Durchführung vierteljährlicher praktischer Angriffs- und Abwehrübungen zum Test der Koordinierung der Notfallmaßnahmen und ihrer kontinuierlichen Verbesserung und Optimierung.

3.7 Datensicherung und Wiederherstellung

ForeNova richtet Datensicherungs- und Notfallwiederherstellungsmechanismen ein, die:

3.7.1 die Durchführung regelmäßiger und automatisierter Datensicherungen zur Gewährleistung der Datenverfügbarkeit und -wiederherstellung im Falle von Datenverlusten/-beschädigungen oder Systemausfällen,

3.7.2 regelmäßige Tests der Datensicherungs- und Wiederherstellungsprozesse beinhalten, um deren Wirksamkeit zu überprüfen.

4. SORGFALTSPRÜFUNGEN BEI UNTERAUFTRAGSVERARBEITERN

4.1 ForeNova unterhält einen Sicherheitsprozess, um vor der Beauftragung von Unterauftragsverarbeitern eine angemessene Sorgfaltsprüfung durchzuführen.

4.2 ForeNova wird mit Unterauftragsverarbeitern eine Datenverarbeitungsvereinbarung schließen, welche die Zuständigkeiten und Pflichten des Auftragsverarbeiters in Bezug auf die Sicherheit eindeutig festlegt, um sicherzustellen, dass die Datenverarbeitung den rechtlichen Anforderungen entspricht.

4.3 ForeNova führt Datenschutz-Audits bei Unterauftragsverarbeitern durch, um sicherzustellen, dass diese die wichtigsten Richtlinien und Standards von ForeNova zur Informationssicherheit einhalten und dass ihre Maßnahmen mindestens ebenso wirksam sind wie diese.

Zusammenfassend gesagt, verfügt ForeNova über ein umfassendes Paket an Maßnahmen zum Datenschutz im Einklang mit den Vorgaben des Standards TOM. Die Kombination aus technischen und organisatorischen Maßnahmen gewährleistet den Schutz sensibler Daten sowie die Einhaltung geltender Vorschriften und bewährter Branchenpraktiken. Zur Aufrechterhaltung eines hohen Maßes an Datenschutz werden diese Maßnahmen regelmäßig bewertet, überwacht und verbessert.