Technische und organisatorische Maßnahmen (TOMs) und technische Lösungsbeschreibung

Version 2.1, Oktober 2024

Versionsfreigabe: Group CTO, General Counsel

Inhaltsverzeichnis

1 Zweck dieses Dokuments

Der Zweck dieses Dokuments besteht darin, die wichtigsten technischen und organisatorischen Maßnahmen (TOMs) zu beschreiben, um die Anforderungen zu erfüllen, die sich aus Art. 32 der Datenschutz-Grundverordnung (DSGVO) und zusätzlich aus den ISMS 27001-Verfahren von Netigate ergeben, um die Sicherheit personenbezogener Daten und anderer Daten in den Diensten von Netigate zu gewährleisten.

1.1 Maßnahmen in der gesamten Gruppe umgesetzt

Die in diesem Dokument beschriebenen TOMs werden in allen Unternehmen der Netigate-Gruppe implementiert, die ihre Software und Dienstleistungen entwickeln und bereitstellen. Die getroffenen Maßnahmen erfüllen die Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit, Risikobewertung, Überprüfung und Belastbarkeit gemäß Art. 32 DSGVO.

1.2 Zusammenfassung der Maßnahmen gemäß Art 32 DSGVO

Netigate hat gemäß Art. 32 DSGVO mindestens folgende Maßnahmen umgesetzt:

a) Zugriffskontrolle und Zugriffsüberprüfung auf der Grundlage der Least-Privilege-Richtlinie und gemäß den Anweisungen des Kunden.
b) Die Anonymisierungsfunktion ist auf Anfrage auf der Plattform verfügbar
c) Datenverschlüsselung während der Übertragung/des Transports und im Ruhezustand.
d) Regelmäßige, verifizierte Backups und Wiederherstellungen
e) regelmäßige Sicherheitstests (Penetrationstests und Schwachstellenanalysen)

2 Einführung eines Produkts/einer Dienstleistung

Netigate und seine Konzerngesellschaften bieten SaaS-Dienste (Software-as-a-Service) an, die zur Erfassung, Analyse und Visualisierung von Feedback-Daten von Kunden oder Mitarbeitern des Kunden verwendet werden. Ein solches Feedback kann beispielsweise aus digitalen Umfragen, öffentlichen Quellen (z. B. Bewertungsseiten, Online-Shops, App Stores) oder internen Systemen des Kunden (z. B. E-Mails aus dem CRM-System, Anrufe aus dem Callcenter oder Chat-Konversationen aus dem Chat-Tool) stammen. Netigate bietet auch Funktionen zum Erstellen und Verteilen von digitalen Umfragen, um durch Kunden-, Mitarbeiter- und Marktforschung Feedback von einer ausgewählten oder kollektiven Gruppe von Befragten zu sammeln. REST-APIs und eine breite Auswahl an Integrationen ermöglichen die Automatisierung von Workflows. Diese Dienste sind browserbasiert und über das öffentliche Internet verfügbar.

Zusätzlich zu den SaaS-Dienstleistungen bietet Netigate auch professionelle Beratungsdienste durch ein Team von internen Beratern an, die sich mit Customer Experience (CX) und Employee Experience (EX) auskennen und eingestellt werden können, um Kunden bei der Gestaltung, Interpretation oder Anwendung von Erkenntnissen und Ergebnissen aus dem gesammelten Feedback zu unterstützen.

3 Risikomanagement

Die Dienstleistungen von Netigate gelten als Dienstleistung mit "normalem Risiko". Wenn der Dienst nur zur Analyse von Daten aus Systemen von Drittanbietern verwendet wird, benötigt er keine personenbezogenen Daten, um die Daten zu verarbeiten. Um Umfragen per SMS oder E-Mail zu verteilen, benötigt der Dienst die Kontaktdaten der Befragten. Die an die Plattform gelieferten Daten werden immer vom Kunden kontrolliert.

Das Information Security Management System (ISMS) von Netigate basiert auf ISO27001 und ist für diese zertifiziert. Der Standard ist risikoorientiert und verwendet eine kontinuierlich aktualisierte Risikoliste, um identifizierte Risiken zu erfassen, zu priorisieren und zu mindern.

Alle Ausnahmen müssen durch ein definiertes Risiko gehandhabt werden, d. h. Sicherheitsrisiken werden gemeldet oder durch Überwachung erkannt, und die daraus resultierende Risikoliste ist ein wichtiger Faktor für die kontinuierliche Arbeit von Netigate zur Risikominderung und -beseitigung. Der Risikoprozess wird vom Sicherheitsteam von Netigate verwaltet und im Rahmen eines monatlichen Sicherheits- und Datenschutzmeetings überprüft.

4 Kontrolle der Privatsphäre

Die Datenschutzkontrollen sind in den Datenschutzrichtlinien des Unternehmens der Netigate-Gruppe beschrieben:

- Zum Analysieren, Visualisieren und Teilen von Ergebnissen: https://lumoa.me/en/privacy-policy.
- Zum Sammeln von Feedback: https://www.netigate.net/legal/

5 Resilienz

Die neuesten Maßnahmen zur Resilienz werden im Bereich *Trust Center* auf der Website von Netigate beschrieben.

5.1 Veränderungsmanagement

Netigate aktualisiert die SaaS-Plattform kontinuierlich und alle Updates werden allen Kunden zur Verfügung gestellt. Wichtige Funktionen oder Änderungen, die von Bedeutung sind, werden den Kunden vor der Bereitstellung mitgeteilt. Netigate verwendet einen klar definierten Secure Development Lifecycle (SLDC), der obligatorische manuelle und automatisierte Tests sowie OWASP-Schwachstellenscans vor der Veröffentlichung umfasst.

5.2 Gehärtete Konfigurationsnorm(en)

Die Konfigurationshärtung erfolgt standardmäßig für alle Umgebungen, wird aber auch mithilfe von CIS-Benchmarks für die Sicherheitsüberwachung für Kubernetes gesteuert. Azure-Clouddienste verfügen über eine hohe Sicherheitsbewertung. Netigate stellt seinen Dienst nur in Azure West Europe (Niederlande, EU) bereit

Ein Großteil der Server wird automatisch in Azure Kubernetes Services (AKS) verwaltet. Der Zugriff auf die Produktionsumgebung ist durch das Prinzip der geringsten Rechte begrenzt und nur einzelne, benannte und identifizierte Benutzer können darauf zugreifen. Multi-Faktor-Authentifizierung.

Entwicklungs-, Test-, Stage- und Production-Umgebungen sind getrennt.

5.2.1 Regelmäßige, dokumentierte Validierung der Konfiguration

Das Entwicklungs- und Betriebsteam verwendet ein automatisiertes Tool, um die Konfiguration für alle Server- und Infrastrukturänderungen regelmäßig und dokumentiert zu validieren. Ausnahmen von der Norm bedürfen einer CTO-Genehmigung. Es gibt ein Verfahren zur Beendigung des Supports, das bei Risikobewertungen berücksichtigt wird.

5.3 Schwachstellen-Management

5.3.1 Flickerei

Netigate patcht seine wichtigsten Software-Frameworks so schnell wie möglich, wenn eine neue Long Time Support (LTS)-Version verfügbar ist. Wir nehmen keine Beta-Versionen in die Produktion, sondern halten an der neuesten LTS-Version fest. Die Patch-Planung erfolgt entlang des normalen Entwicklungs-/Betriebsplanungsprozesses. Dieser Prozess findet in 2-wöchigen Sprint-Zyklen statt, in denen das Planungsmeeting einen neuen Sprint startet.

5.3.1.1 Regelmäßiges Patchen

Das regelmäßige Patchen der Produktionsumgebung wird kontinuierlich für die Patches durchgeführt, die keine Unterbrechungen der Systemnutzung verursachen, und das Patch-Fenster für Patches, die innerhalb des Wartungsfensters ausfallen oder einen geplanten Ausfall mitteilen können.

Das Patchen der TEST-Umgebung muss mindestens 24 Stunden vor Beginn des Patch-Fensters für die Produktionsumgebung abgeschlossen sein. Akzeptanzkriterien für das Patchen sind unsere automatisierten und manuellen Tests, in der Regel wird der Patch einer neuen Softwareversion mindestens einige Tage in der TEST-Umgebung aufbewahrt, bevor der Patch in der Produktion angewendet wird.

5.3.1.2 Notfall-Patching

Im Falle einer kritischen Schwachstelle, die vom Anbieter erkannt / angekündigt wird und bei der die Auswirkungen durch das Warten auf ein regelmäßiges Patching-Fenster als hoch eingestuft werden, wird ein Notfall-Patching-Fenster geplant. Die Entscheidung, ob Patches im Notfall-Patching-Fenster implementiert werden sollen, wird vom Netigate CTO getroffen.

5.3.1.3 Regelmäßige Validierung des Patchings

Serverkonfigurationen und Patch-Level werden regelmäßig überprüft. Die Validierung erfolgt durch das Entwicklungs- und Betriebsteam unter Verwendung automatisierter Tools, um Schwachstellen zu erkennen und zu überwachen .

5.3.1.4 Ausnahmen beim Patchen

Falls eine Ausnahme für einen Patch erforderlich ist, muss dieser vom Entwicklungsteam über Netigate CTO genehmigt werden.

5.3.2 Viren- / Malware-Erkennung

Die Informationssicherheitsrichtlinie von Netigate verlangt, dass auf allen Computern von Netigate eine aktuelle Antiviren-/Malware-Software installiert und auf dem neuesten Stand ist. Alle unsere Workloads befinden sich in Azure und sind durch Azure Defender geschützt. Dazu gehören Speicherscans auf potenzielle Malware, Container-Registry auf anfällige Images, Überwachung auf verdächtige Aktivitäten sowohl auf virtuellen Maschinen als auch auf Kubernetes-Clustern usw.

5.3.3 Schwachstellen-Scanning

OWASP-Code und Abhängigkeiten Schwachstellenscans werden regelmäßig für jeden Software-Build durchgeführt. Darüber hinaus werden Penetrationstests und Sicherheitsaudits von Drittanbietern, die von der Personalabteilung durchgeführt werden, mindestens einmal pro Jahr durchgeführt. Die Überprüfung von Schwachstellen in der Infrastruktur erfolgt mit Azure Security Center.

Alle validierten Befunde, die gefunden werden konnten und kritische/hohe Schwachstellen darstellen, werden sofort entschärft und eine dauerhafte Lösung für sie entwickelt. Niedrigere Sicherheitsprobleme werden ebenfalls über die Funktionalität gestellt, um die Systemsicherheit hoch zu halten.

Bericht(e) werden gemäß Netigate ISMS gespeichert. Zuletzt wurden Sicherheitstests, Scanning + Intrusion Testing durchgeführt. Der Prozess für den Drittanbieter wird so durchgeführt, dass 2 Testrunden durchgeführt werden und alle gefundenen Probleme behoben werden oder das Systemverhalten dem Drittanbieter erklärt wird, mit dem Endziel, keine Probleme zu haben. Berichte sind auf Anfrage erhältlich.

Netigate verpflichtet sich, regelmäßig interne Schwachstellenscans durchzuführen, und für intern gefundene Schwachstellen bemühen wir uns, den folgenden Zeitplan für die Behebung einzuhalten

- Zero-Day-Schwachstelle: So schnell wie möglich
- Kritisches Risiko: 30 Tage
- Hohes Risiko: 90 Tage
- Mittleres Risiko: Kein Zeitlimit

5.4 Protokollverwaltung und Prüfpfade

Im Folgenden wird definiert, wie Benutzerzugriffe (z. B. Zugriff anzeigen, ändern, löschen) regelmäßig protokolliert und überwacht und unbefugte Zugriffe oder verdächtige Benutzeraktivitäten entsprechend gekennzeichnet werden.

5.4.1 Betriebssystem

Protokolle innerhalb des Netigate-Betriebssystems werden gemäß den Best Practices der Branche konfiguriert und Netigate befolgt ISO27001.

5.4.2 Anwendung

Netigate protokolliert alle Ereignisse in einem zentralen Protokollierungssystem, das sich in der EU befindet.

Eine Protokolldatei enthält beispielsweise in der Regel Folgendes:

- DATUM + Zeitstempel
- LEVEL, "Warnung, Fehler, Info"
- GASTGEBER
- DIENST
- CONTENT (tatsächlicher Text des Protokolls)

Anwendungsprotokolle werden überhaupt nicht gelöscht, um die Daten im Falle von Vorfällen zu überprüfen. Wir protokollieren dort auch keine sensiblen Daten (siehe Kapitel Personenbezogene Daten in Protokollen). Der Zugriff auf Protokolle wird nur ausgewählten Betriebsmitarbeitern gewährt, die eine 2-Faktor-Authentifizierung und persönliche Benutzer erfordern.

Netigate protokolliert Benutzeraktivitäten wie Logins und Datenexporte oder Uploads. Alle Dienste protokollieren ihre Aktionen in Info-Level-Protokollen und sollten Warnungen oder Fehler auftreten, werden diese ebenfalls gespeichert.

Netigate hat die notwendigen Alarme auf der Grundlage von Protokollen eingerichtet. Diese werden täglich überwacht.

5.4.3 Zeitsynchronisation

Bei allen Integrationsservern ist der Zeitsynchronisierungstyp so eingestellt, dass er mit dem Domänencontroller in UTC-Zeit synchronisiert wird.

5.4.4 Personenbezogene Daten in Protokollen

Personenbezogene Daten werden nicht in unsere Protokolle aufgenommen, wir verwenden eine interne Benutzer-ID anstelle von Benutzernamen, E-Mail usw. Mail. Bei Umfrageantworten wird in Webproxy-Protokollen die öffentliche IP-Adresse 1 Woche lang gespeichert, um Angriffe zu identifizieren und abzuwehren. IP-Adressen werden niemals in Kombination mit anderen Daten gespeichert.

6 Schutz personenbezogener Daten

6.1 Richtlinie zur Verschlüsselung

Wir befolgen https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
, um TLS-Verschlüsselungen zu bewerten, die zur Sicherung der Kommunikation zwischen unseren Servern und Kundenbrowsern/-integrationen verwendet werden. Obwohl wir uns

bemühen, die bestmögliche Abwärtskompatibilität zu bieten, unterstützen wir auch keine Verschlüsselungen, die als schwach eingestuft werden. Netigate unterstützt derzeit TLS 1.2 und TLS 1.3

6.2 Verschlüsselung ruhender Daten und Pseudonymisierung

Gemäß der Informationssicherheitsrichtlinie von Netigate verschlüsselt Netigate alle eingeschränkten Benutzerdaten im Ruhezustand durch sichere Verschlüsselungsalgorithmen und Bibliotheken.

Zum Beispiel werden vom Benutzer erstellte Passwörter durch eine unidirektionale BCrypt-Verschlüsselung mit mindestens 2048 Iterationen und einzigartigem benutzerspezifischem Salt verschlüsselt. Neben der Einarbeitung eines Salzes zum Schutz vor Regenbogentischangriffen. Es ist nicht möglich, die Passwörter zu entschlüsseln, um sie in ihre ursprüngliche Form zurückzuversetzen. Der Zugriff auf Kundendaten ist streng nach Bedarf eingeschränkt.

Für alle ruhenden Daten wird eine AES-Festplattenverschlüsselung von mindestens 256 Bit verwendet, und wo immer möglich, beschränken wir den Zugriff auf verwaltete Instanzen für das Personal des Cloud-Anbieters.

6.3 Verschlüsselung während der Übertragung

Die gesamte Kommunikation zu und von Netigate-Diensten, externen Diensten und Benutzern erfolgt über das HTTPS-Protokoll.

Der API-Schlüssel wird für die Authentifizierung eingehender Anfragen an den Netigate-Dienst verwendet, um auf die öffentlichen Endpunkte von Netigate pro Client und Sammlungsbasis zuzugreifen. Jeder Client wird mit einer unternehmens- und sammlungsspezifischen ID versehen, Administratoren können auf die Liste der API-Schlüssel zugreifen

7 Vertraulichkeit

In den folgenden Abschnitten werden die Ebenen und die Art des Zugriffs beschrieben, die Benutzern basierend auf der Vertraulichkeit der Daten und dem legitimen Geschäftsbedarf der Benutzer für den Zugriff auf personenbezogene Daten bereitgestellt werden.

7.1 Verwaltung von Admin-Rechten

Der Zugriff auf die Server wird von Netigate verwaltet, es werden immer persönliche Konten verwendet. Die Verwendung von gemeinsam genutzten Konten ist nicht erlaubt und die Privilegien werden nach dem Prinzip der geringsten Rechte vergeben.

Normalerweise haben nur Mitglieder des Infrastrukturteams Zugriff auf Server, aber für zeitlich begrenzte Aufwände können vorübergehend erhöhte Berechtigungen erteilt werden. In diesem Fall wird der Zugriff nur auf eine bestimmte Umgebung (Test, Stage, Prod) gewährt.

7.1.1 Regelmäßige Validierung der Admin-Rechte

Der erhöhte Zugriff wird im Rahmen des ISMS von Netigate in den Sicherheits- und Datenschutzbesprechungen regelmäßig überprüft. Rollen werden überprüft und entfernt, wenn sie nicht mehr benötigt werden. Die Validierung erfolgt mithilfe einer manuellen Benutzerbeendigungsaktion.

Berichte von einzelnen Validierungen werden in Besprechungsprotokollen von wiederkehrenden Sicherheitsbesprechungen gespeichert.

7.2 Verwaltung privilegierter Benutzer

Für jeden Datensatz/Mandanten wird ein individuelles Token für den API-Zugriff erstellt. Für Analysen erhält jeder Benutzer Zugriff auf einen bestimmten Datensatz. Netigate erfordert derzeit keine 2-Faktor-Authentifizierung, kann aber über SSO eingerichtet werden.

7.3 Überwachung

Netigate verwendet eine Kombination von Diensten, um Protokollierung, Überwachung und Warnungen bereitzustellen. Warnungen sind so konfiguriert, dass Warnungen ausgegeben werden, wenn beispielsweise sowohl das Gesamtsystem als auch bestimmte Komponenten oder Prozesse ausfallen oder kurz vor dem Fehlschlagen stehen oder Anmeldeversuche fehlgeschlagen sind.

Der Webproxy wird verwendet, verarbeitet und protokolliert alle eingehenden Anfragen, die an die Server gelangen. Darüber hinaus protokolliert Netigate fehlgeschlagene Anmeldeversuche und alle API-Anfragen. Netigate speichert sowohl Aktivitätsprotokolle als auch Ressourcenprotokolle von Vorgängen, die im Cloud-Anbieter und auf den Ressourcen des Cloud-Anbieters ausgeführt werden.

Überwachung und Protokolle sind auf privilegierte Benutzer auf verschiedenen Ebenen beschränkt, je nachdem, ob sie darauf zugreifen müssen, um einen funktionalen und sicheren Dienst bereitzustellen.

8 Integrität

Datenintegrität ist ein weit gefasstes Konzept, und es werden verschiedene Maßnahmen ergriffen, um sie zu gewährleisten. Zunächst werden die Daten validiert, wenn sie an Netigate übertragen werden. Zweitens werden Zugriffs- und Schreibvorgänge in Datenbanken eingeschränkt, und drittens stellen Backups sicher, dass die Daten in ihren ursprünglichen Zustand zurückversetzt werden können.

9 Verfügbarkeit

Die Datenverfügbarkeit wird durch Redundanz der meisten (aber nicht aller) unserer Dienste sichergestellt. Alle Dienste werden überwacht und an die Produktteams zur Abhilfe gewarnt.

10 Möglichkeit zur Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten

Im Folgenden wird definiert, wie die Verfügbarkeit, unbefugte oder versehentliche Zerstörung personenbezogener Daten kontrolliert wird

10.1 Business Continuity und Disaster Recovery

Business Continuity und Disaster Recovery werden in Netigates Business Continuity Plan and Incident Management Procedure beschrieben, die Teil der ISMS-Dokumentation von Netigate sind.

10.1.1 Validierung von Disaster Recovery-Tests

Disaster Recovery-Tests werden alle zwei Jahre durchgeführt und die Ergebnisse werden im Netigate-Ticketsystem gespeichert.

10.2 Datensicherung und -wiederherstellung

Datenbankserver werden mindestens mit der folgenden Konfiguration gesichert:

- Wöchentliche Voll-Backups
- Inkrementelle, stündliche Sicherungen
- Speicherung:
    - Kurzfristig: 7 Tage
    - Langfristige, gekühlte Lagerung: 6 Monate
- Redundanz: 2. Region

Alle Produkt- und Infrastrukturdaten werden separat gespeichert und alle Umgebungen können bei Bedarf in einer neuen Region neu erstellt werden.

10.2.1 Validierung von Tests zur Datensicherung und -wiederherstellung

Wiederherstellungstests werden im Rahmen des ISMS mindestens alle 6 Monate durchgeführt.

11 Softwaremanagement und Schwachstellenmanagement

11.1 Anwendungsumgebung

11.1.1 Abhängigkeiten und Malware

Abhängigkeiten von 3rd-Party- und Open-Source-Software für die Anwendungsentwicklung und -laufzeit werden im Code definiert und während der Builds gescannt, bevor sie in der Produktion bereitgestellt werden. Diese Abhängigkeiten werden von Github Dependabot, Continuity Sonarcloud und Azure Container Registry gescannt, um potenzielle Schwachstellen zu erkennen.

11.1.2 Schwachstellen-Management

Potenzielle Sicherheitsrisiken werden während des Builds gemeldet, und der anfällige Build wird abgebrochen. Kritische Schwachstellen müssen in der Test- und Staging-Umgebung innerhalb von 1 Arbeitstag und in der Produktionsumgebung innerhalb von 2 Arbeitstagen gepatcht werden.

Vorhandene Builds werden täglich von Azure Security Center überprüft, und es werden kritische Sicherheitsrisiken gemeldet.

11.2 Server-Umgebung

11.2.1 Code-Review für installierte Software

Wenn Software auf Servern installiert ist, sollte dies in Code definiert werden, der Code-Reviews in Konfigurationsmanagement-Software unterliegt, z. B. Puppet, Chef, Ansible.

11.2.2 Installation und Versionierung

Die Installation und Versionen von Software-as-a-Service werden mit Infrastruktur als Code-Software Terraform definiert, und Änderungen können überprüft werden.

11.2.3 Überwachung von Schwachstellen

Sicherheitsrisiken werden mithilfe von Azure Security Center überwacht. Kritische Schwachstellen müssen in der Test- und Staging-Umgebung innerhalb von 1 Arbeitstag und in der Produktionsumgebung innerhalb von 2 Arbeitstagen gepatcht werden.

11.3 Arbeitsplatz und mobile Endgeräte der Mitarbeiter

Die Softwareinstallation und das Schwachstellenmanagement sind in der Richtlinie für mobile Geräte definiert.

12 Sicherheit der Kommunikation

12.1 Verwaltung der Netzwerksicherheit

12.1.1 Steuerung des Netzwerks

Alle Netzwerkkonfigurationen und -richtlinien werden mit Infrastruktur als Code-Software Terraform definiert, und Änderungen können überprüft werden.

Anwendungsumgebungen (Tests, Staging und Produktion) enthalten nur Funktionen, die für die Anwendungsfunktionalität unbedingt erforderlich sind.

Mitarbeiterzugriff auf CI/CD-Tools, Anwendungsumgebung, Datenbankzugriff nur über VPN mit Audit-Log möglich. Darüber hinaus sollte die gesamte interne und externe Kommunikation mit applicationauth-Umgebungen über TLS gesichert werden.

Die interne Netzwerksicherheit wird aktiv durch Azure Defender Intrusion Detection geschützt.

12.1.2 Sicherheit von Netzwerkdiensten

Die Netzwerksicherheit der Anwendungsumgebung entspricht den Empfehlungen des Azure Security Center, die mehrere standardmäßige Konformitätsberichte enthalten. Diese Berichte werden regelmäßig überprüft und die notwendigen Empfehlungen werden vom Entwicklungsteam umgesetzt.

12.1.3 Segregation in Netzwerken

VPN-Server, CI/CD-Tools, Produktions-, Staging- und Testumgebungen sind in separate Netzwerke unterteilt. Diese Netzwerke sind von anderen Netzwerken isoliert, die für alltägliche Aufgaben verwendet werden – Internetzugang der Mitarbeiter, Dokumentenspeicherung usw.

Die öffentliche HTTPS-Terminierung für Anwendungsumgebungen wird für alle Anwendungen über den Kubernetes-Eingangscontroller zentralisiert. Dies ermöglicht eine zentralisierte Verwaltung und Konfiguration von öffentlichen TLS-Zertifikaten.

12.2 Sitzungen

Die Sitzungsverwaltung variiert je nach Vertraulichkeit der Daten. Für den Zugriff auf Funktionen, die keine personenbezogenen Daten sind, beträgt der Sitzungsablauf 30 Tage (bei Inaktivität oder Abmeldung)

In administrativen Teilen, in denen personenbezogene Daten erfasst werden, beträgt die Standardsitzungszeit 30 Minuten.

12.3 Informationstransfer

12.3.1 Richtlinien und Verfahren für die Informationsübertragung

Das Messaging zwischen Anwendungsdiensten, Teilen der Anwendungsinfrastruktur sowie zwischen Netigate-Anwendungen und Benutzern erfolgt nur über verschlüsselte Kanäle. Die bevorzugte Verschlüsselung sollte TLS mit der Protokollversion 1.3 oder 1.2 mit bekannten und sicheren Cipher Suites sein.

Die gesamte E-Mail-Kommunikation, einschließlich Anhänge, unterliegt dem Spam-Schutz eines Malware-Scans. Alle Dokumente, die über Netigate-Anwendungen hochgeladen werden, unterliegen einem Malware-Scan.

12.3.2 Vereinbarungen über die Informationsübermittlung

Es gibt zwei wichtige externe APIs, die Netigate-Kunden zur Verfügung stehen:

- für die Bereitstellung externer Daten für den Insights- und Analytics-Teil der Plattform oder für den Export von Daten https://help.lumoa.me/en/articles/525-api-documentation
- Umfragen, Befragten- und Antwortdaten können über die Feedback-Kunden-API abgerufen und hinzugefügt werden: https://api.netigate.net/v1.2/index.html.

Kunden können bei Bedarf auch manuell Daten in/aus der Netigate-Benutzeroberfläche von/nach Excel importieren und exportieren.

Netigate kann bei Bedarf auch dabei helfen, eine benutzerdefinierte Integration einzurichten und dafür einen separaten Vertrag abzuschließen. Die benutzerdefinierte Integration kann verwendet werden, um Daten vom vom Kunden bereitgestellten Endpunkt abzurufen.

12.3.3 Elektronische Nachrichten

Die Kommunikation außerhalb der Netigate CX-Anwendung mit den Benutzern kann über E-Mail, GSM oder Festnetztelefonie erfolgen.

12.3.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Die überwiegende Mehrheit der Verträge zwischen Unternehmen der Netigate-Gruppe und Kunden basiert auf Unternehmensvorlagen/Standardbedingungen, nicht auf denen des Kunden, und enthält marktübliche Vertraulichkeitsklauseln. Für Auftragnehmer und Mitarbeiter, die ein Unternehmen der Netigate-Gruppe sind, wird eine Standardvorlage verwendet, die auch eine marktübliche Vertraulichkeitsklausel enthält, die den Schutz aller Kundendaten beinhaltet.

13 Physische Sicherheit

Der Zugang zu den physischen Einrichtungen von Netigate ist durch persönliche Schlüsselkarten + geheime PIN geschützt. Darüber hinaus werden sensible Bereiche wie Netzwerk, juristische Dokumente und die interne IT durch zusätzliche elektronische Schlösser geschützt. Jeder Zugriff (erfolgreich oder versucht) wird überwacht, gewarnt und protokolliert.

Netigate nutzt mehrere Cloud-Anbieter wie Azure und Aiven für die Server-, Netzwerk- und Speicherinfrastruktur. Alle sind nach der Norm ISO 27001 zertifiziert, die sich klar auf z.B. Zutrittskontrolle, physische Sicherheit und den Umgang mit physischen Medien und Geräten konzentriert.

Weitere Informationen zur physischen Sicherheit von Azure und zur Handhabung von physischem Speicher finden Sie unter:

- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

14 Anonymisierung

Die Datenschutzrichtlinie von Netigate beschreibt, wie wir mit personenbezogenen Daten (PII) umgehen, die von Netigate gesammelt werden.

- Informationen der Befragten, die von dem Unternehmen, das die Umfrage durchführt (der Verantwortliche für die Datenverarbeitung), zur Verfügung gestellt werden, meistens Ihre E-Mail-Adresse und Telefonnummer, aber auch zusätzliche Informationen wie organisatorische oder regionale Zugehörigkeit
- Umfrageantworten oder andere Formen von Feedback-Metadaten zu Umfrageantworten wie Uhrzeit und Datum der Beantwortung

Die Produkte von Netigate bieten viele Möglichkeiten, die Erfassung personenbezogener Daten zu verhindern, anonyme Ergebnisse mit einer Person in Verbindung zu bringen und die DSGVO-konforme Entfernung personenbezogener Daten zu gewährleisten. Einige Beispiele sind:

- Anonyme Umfrage-Links
- Mindestanzahl von 3 Teammitgliedern, um aggregierte Daten anzuzeigen
- Geplante Entfernung aller Antwortdaten oder Kontaktdaten und nur offener Antworten
- Automatisierte Entfernung personenbezogener Daten vor der Verarbeitung durch öffentliche ML-Modelle.

Darüber hinaus werden personenbezogene Netzwerkdaten, wie z. B. I-Adressen, von personenbezogenen Daten getrennt und niemals mit personenbezogenen Daten gespeichert.

15 Unterauftragsverarbeiter

Netigate beauftragt Unterauftragsverarbeiter wie z. B. Rechenzentrumsbetreiber mit der Erbringung der Dienste und der Verarbeitung von Daten im Namen von Netigate und seinen Kunden. Die Rechenzentren des Unterauftragsverarbeiters sind mindestens nach ISO 27001 zertifiziert. Die aktuellen Unterauftragsverarbeiter von Netigate sind in der Liste der Unterauftragsverarbeiter aufgeführt, die unter www.netigate.net/legal verfügbar ist. Dokumentationen über technische und organisatorische Maßnahmen des jeweiligen Unterauftragsverarbeiters sind auf Anfrage erhältlich.