nonimo

SICHERHEITS-WHITEPAPER

Nonimo Gateway und DSGVO: das Whitepaper für Ihren DSB

Was mit einem Text geschieht, der über Nonimo Gateway an einen KI-Anbieter geht: Ort, Zugriffe, Speicherung, Löschung und Rollen, aufbereitet für die Prüfung durch Datenschutz, IT und Recht.

Das Nonimo-Team
November 2026 nonimo.eu

SICHERHEITS-WHITEPAPER

Nonimo Gateway und DSGVO: das Whitepaper für Ihren DSB

Was mit einem Text geschieht, der über Nonimo Gateway an einen KI-Anbieter geht: Ort, Zugriffe, Speicherung, Löschung und Rollen, aufbereitet für die Prüfung durch Datenschutz, IT und Recht.

Das Nonimo-Team · November 2026 · 13 Min. Lesezeit

Das finden Sie darin

- Die Kurzfassung auf einer Seite für Ihre Datenschutzbeauftragten
- Der Weg eines Textes von Ihrer Anwendung bis zum KI-Anbieter und zurück
- Die vertrauliche Maschine in Irland: was sie ist und was sie zusagt
- Was verschlüsselt gespeichert wird und in welchen vier Fällen es gelöscht wird
- Rollen nach DSGVO: Verantwortlicher, Auftragsverarbeiter, Unterauftragsverarbeiter
- Monatsbericht und Protokoll je Anfrage als Nachweis für VVT und DSFA
- Zwölf Fragen, die Ihr DSB uns stellen kann, mit kurzer Antwort

Das Wichtigste in Kürze

- Bevor eine Anfrage beim KI-Anbieter ankommt, ersetzt Nonimo Gateway Namen, Firmen, Ausweisnummern, Konten und Kontaktdaten durch Platzhalter.
- Jeder Kunde erhält eine eigene vertrauliche Maschine von Microsoft Azure in Irland; was sie verarbeitet, wird von Mitarbeitenden von Nonimo und Microsoft nicht gelesen.
- Der Text macht seinen Weg und bleibt nicht liegen. Gespeichert werden nur Einstellungen, Ihr Anbieterschlüssel und eigene Begriffe, verschlüsselt.
- Nonimo erhält ausschließlich Zahlen. Ihr DSB bekommt einen Monatsbericht und ein Protokoll je Anfrage, beide ohne einen einzigen Datenwert.

01

Die Kurzfassung für Ihre Datenschutzbeauftragten

Dieses Whitepaper beantwortet die Fragen, die eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter stellt, bevor eine Fachabteilung Texte mit Kundendaten an einen KI-Dienst schicken darf. Es beschreibt, was Nonimo Gateway leistet und welche Zusagen wir machen. Für die datenschutzrechtliche Bewertung zählen Ort, Zugriffe, Speicherdauer und Rollen; dazu finden Sie hier belastbare Angaben.

Nonimo Gateway sitzt zwischen den Anwendungen Ihres Unternehmens und dem KI-Anbieter, den Sie selbst ausgewählt haben. Bevor eine Anfrage hinausgeht, erkennt es die personenbezogenen Daten darin (Namen, Unternehmen, Ausweis- und Steuernummern, Bankverbindungen, E-Mail-Adressen und Telefonnummern) und setzt an ihre Stelle Platzhalter wie `[PERSON_1]` oder `[IBAN_1]`.

Kommt die Antwort zurück, stehen die echten Daten wieder an ihrem Platz. Ihre Mitarbeitenden lesen einen ganz normalen Text.

Die wichtigsten Punkte auf einen Blick:

Frage	Antwort
Wo wird verarbeitet?	Auf einer vertraulichen Maschine von Microsoft Azure in Irland, die nur Ihrem Unternehmen dient
Wer kann den Text lesen?	Ihre Anwendungen und, mit Platzhaltern statt Daten, Ihr KI-Anbieter. Mitarbeitende von Nonimo und Microsoft lesen ihn nicht
Was erhält Nonimo?	Zahlen: Anzahl der Anfragen und der ersetzten Daten, dazu die Lizenzverlängerung
Was wird gespeichert?	Ihre Einstellungen, der Schlüssel Ihres KI-Anbieters und Ihre eigenen Begriffe, verschlüsselt und in derselben Region
Und der Text selbst?	Er wird nur durchgeleitet und nirgends abgelegt
Wann wird gelöscht?	Im Test nach drei Tagen ohne Nutzung, am Ende der Testphase ohne Tarif, am Ende des Abonnements oder auf Ihren Wunsch
Welche Unterlagen bleiben?	Ein Monatsbericht für den DSB und ein Protokoll je Anfrage, beide nur mit Zahlen

Den Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO stellen wir Ihnen auf Anfrage an hello@nonimo.ai zur Verfügung.

02

Der Weg eines Textes durch Nonimo Gateway

Nehmen wir einen einfachen Fall. Die Buchhaltung der Musterfirma GmbH lässt Mahnschreiben von einem Sprachmodell formulieren. Bisher schickte die interne Anwendung den Entwurf mit Name, Bankverbindung und Steuer-ID direkt an den KI-Anbieter. Mit Nonimo Gateway ändern sich in der Anwendung nur Zieladresse und Zugangsschlüssel. Der Weg sieht dann so aus:

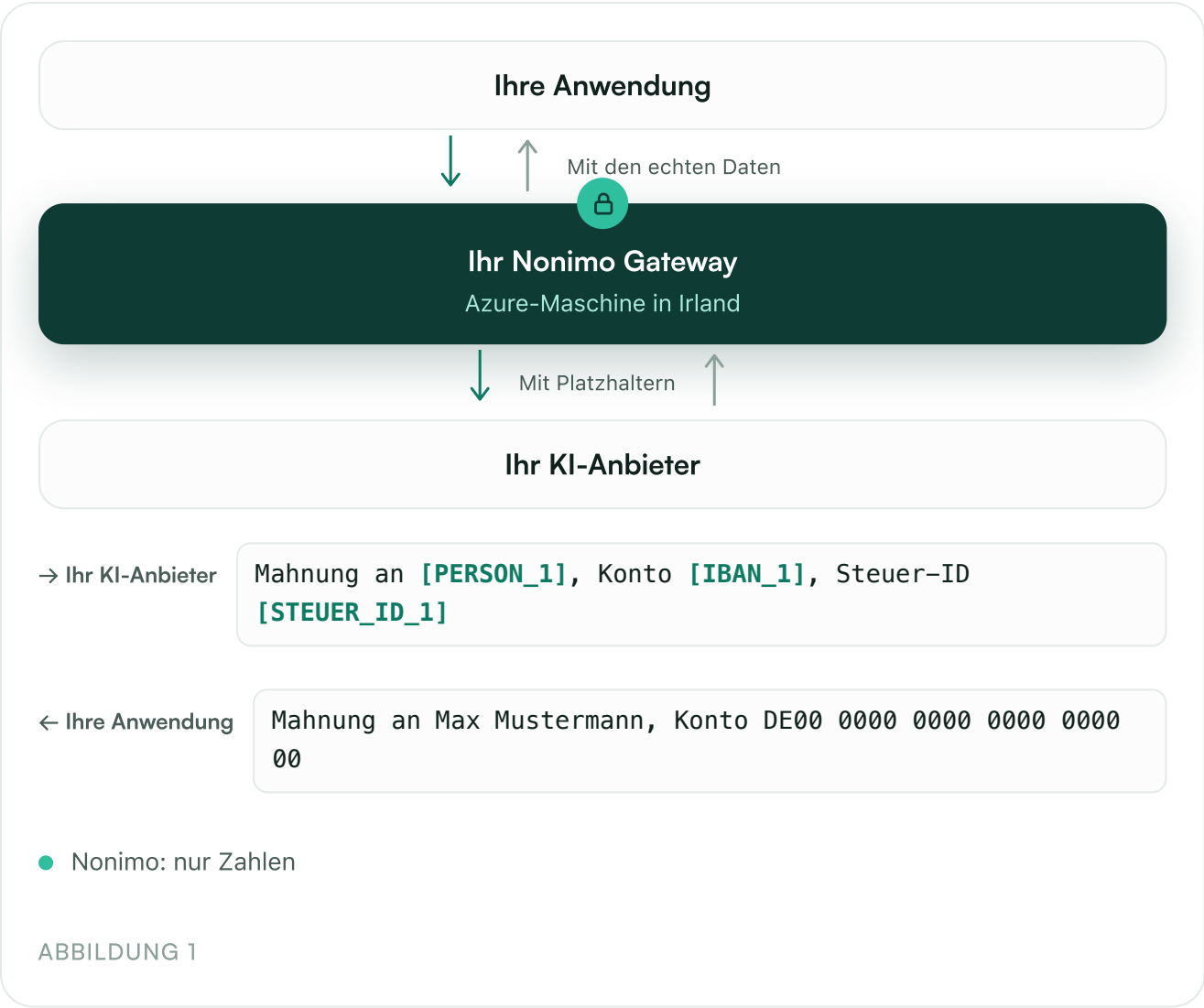

ABBILDUNG 1

1. **Ihre Anwendung** sendet die Anfrage über HTTPS an die eigene Adresse Ihres Gateways, mit einem eigenen Zugangsschlüssel.
2. **Ihr Gateway** ersetzt auf der vertraulichen Maschine in Irland jeden erkannten personenbezogenen Wert durch einen Platzhalter. Aus „Mahnung an Max Mustermann“ wird `Mahnung an [PERSON_1]`.
3. **Ihr KI-Anbieter** erhält die Anfrage mit Platzhaltern, verarbeitet sie mit Ihrem eigenen Schlüssel und schickt die Antwort zurück.
4. **Ihr Gateway** setzt die echten Daten wieder ein, bevor die Antwort Ihre Anwendung erreicht.

Das gilt auch dann, wenn die Antwort gestreamt wird, also Stück für Stück ankommt, und wenn das Modell Werkzeuge aufruft (Tool Calls). Ihre Nutzer sehen fließenden Text mit den richtigen Namen, Ihr KI-Anbieter sieht Platzhalter.

Für jede Datenart legen Sie fest, was geschehen soll: ersetzen, die Anfrage anhalten oder nur einen Hinweis geben und mitzählen. So kann etwa eine Kanzlei bestimmen, dass Anfragen mit einer Steuer-ID gar nicht erst hinausgehen, während Namen ersetzt werden. Zusätzlich hinterlegen Sie im Dashboard eigene Begriffe wie Mandanten- oder Projektnamen; sie werden genauso behandelt.

Nonimo Gateway spricht die Schnittstellen, die Ihre Entwickler bereits nutzen: die API von OpenAI (Chat Completions und Responses) und die von Anthropic (Messages). Das offizielle SDK, die Modelle, die Nachrichten und die Programmlogik bleiben, wie sie sind. Damit lassen sich Anbieter wie OpenAI und Claude (Anthropic) anbinden.

> **Hinweis:** Als Unternehmen erhält Nonimo ausschließlich Zahlen: wie viele Anfragen durchgelaufen sind und wie viele Daten ersetzt wurden. Der Text geht von Ihrer Anwendung über die vertrauliche Maschine zu Ihrem KI-Anbieter und zurück.

03

Wo Ihr Gateway läuft und wer darauf zugreifen kann

Jedes Unternehmen erhält eine eigene vertrauliche Maschine von Microsoft Azure in der Region Irland, also innerhalb der Europäischen Union. Sie wird mit keinem anderen Kunden geteilt.

„Vertraulich" ist hier ein Fachbegriff aus dem Confidential Computing. Nonimo Gateway nutzt die vertraulichen Container von Azure auf Basis von AMD SEV-SNP. Dabei verschlüsselt der Prozessor selbst den Arbeitsspeicher der Maschine.

Was dort verarbeitet wird, bleibt auch gegenüber den Betreibern der Cloud verschlüsselt. Es handelt sich um öffentlich dokumentierte Technik von Microsoft, die Ihre IT in der Azure-Dokumentation nachlesen kann [5].

Für Sie ergeben sich daraus drei Zusagen:

- **Eigene Maschine:** Ihr Gateway läuft auf einer Maschine, die nur Ihrem Unternehmen dient, in Irland.
- **Nur veröffentlichte Versionen:** Die Maschine startet ausschließlich veröffentlichte Versionen von Nonimo Gateway.
- **Geschlossenes Gateway:** Was Ihr Gateway verarbeitet, wird von Mitarbeitenden von Nonimo und Microsoft nicht gelesen.

Für Ihre Dokumentation heißt das: Der Ort der Verarbeitung ist eindeutig benannt und liegt in der EU. Die echten Daten im Klartext gibt es nur in Ihren eigenen Systemen und auf Ihrer vertraulichen Maschine.

04

Was gespeichert wird und wann es gelöscht wird

Ein Gateway braucht einige wenige Angaben, um für Sie zu arbeiten. Diese Angaben speichert es verschlüsselt und in derselben Region wie die Maschine:

- Ihre **Einstellungen**, etwa welche Datenarten ersetzt, angehalten oder nur gemeldet werden;
- den **Schlüssel Ihres KI-Anbieters**, den Sie selbst hinterlegen;
- die **eigenen Begriffe**, die Sie hinzugefügt haben.

Entschlüsseln kann diese Angaben nur Ihre eigene Maschine, wenn sie eine veröffentlichte Version des Gateways ausführt. Sie bleiben bei Neustarts und Updates erhalten, sodass Sie nichts neu einrichten müssen.

Der Text Ihrer Anfragen und Antworten gehört nicht dazu. Er macht seinen Weg und bleibt nicht liegen. Auch die Zuordnung zwischen Platzhaltern und echten Werten existiert nur im Arbeitsspeicher, solange die Anfrage läuft, und wird nie auf einen Datenträger geschrieben.

Das vereinfacht Ihre Löschkonzepte erheblich: Für die Inhalte, die über das Gateway laufen, entsteht beim Gateway kein Bestand, der aufbewahrt, gesichert oder später gelöscht werden müsste.

Für das Gateway selbst gibt es vier klar definierte Löschanlässe:

1. **Drei Tage in Folge ohne Nutzung während des Tests.** Einen Tag vorher erhalten Sie einen Hinweis.
2. **Ende der Testphase** ohne gebuchten Tarif.
3. **Ende des Abonnements.**
4. **Auf Ihren Wunsch**, jederzeit.

Mit dem Gateway werden auch die gespeicherten Einstellungen, Schlüssel und Begriffe entfernt.

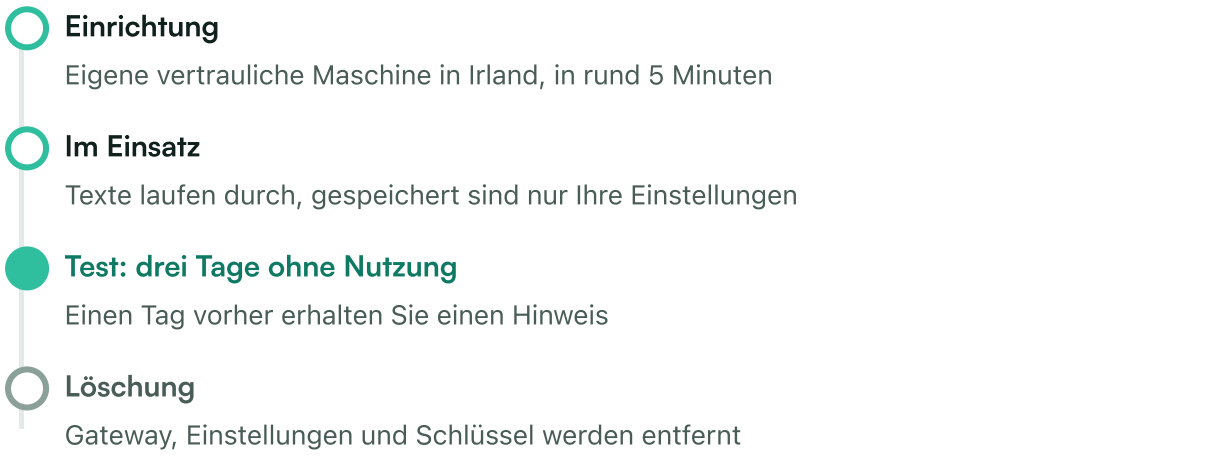

ABBILDUNG 2

05

Zugänge, Schlüssel und das Entwicklerwerkzeug

Bei einem Dienst, der zwischen Ihren Anwendungen und einem KI-Anbieter steht, will die IT-Leitung wissen, welche Schlüssel es gibt und wer sie in der Hand hat. Bei Nonimo Gateway sind es drei, sauber getrennt:

Schlüssel	Wofür	Wer ihn hat
Zugangsschlüssel des Gateways	Ihre Anwendungen melden sich damit an der eigenen Adresse Ihres Gateways an	Ihr Unternehmen
Schlüssel des Dashboards	Zugang zu Einstellungen, Bericht und Protokoll	Ihr Unternehmen, getrennt vom Zugangsschlüssel
Schlüssel Ihres KI-Anbieters	Das Gateway leitet damit die Anfragen mit Platzhaltern weiter	Ihr Unternehmen; Sie fügen ihn selbst auf der Seite Ihres Gateways ein

Alle Verbindungen von Ihren Anwendungen zum Gateway laufen über HTTPS. Bei der Einrichtung erhalten Sie den Zugangsschlüssel und den Schlüssel des Dashboards und bewahren beide auf. Den Vertrag mit dem KI-Anbieter schließen Sie selbst, und die Anfragen laufen über Ihr eigenes Konto.

Viele Teams lassen sich heute beim Programmieren von einem KI-Assistenten helfen. Dafür gibt es einen lokalen MCP-Connector, der auf dem Rechner der Entwicklerin oder des Entwicklers läuft.

Der Assistent kann damit den Zustand des Gateways abfragen, die Schlüssel nach Bestätigung durch die Person in der Konfiguration ablegen, die Stellen im Code finden, an denen der KI-Anbieter aufgerufen wird, die Umstellung vorschlagen, einen Test mit erfundenen Daten fahren und den Bericht für den DSB herunterladen.

Die Schlüssel gehen dabei vom Rechner Ihres Teams direkt zu Ihrem Gateway, ohne über Nonimo zu laufen.

06

Wer welche Rolle hat

Für das Verzeichnis von Verarbeitungstätigkeiten und den Vertrag zur Auftragsverarbeitung braucht Ihr DSB eine klare Rollenverteilung. Für die Texte, die über das gehostete Gateway laufen, sieht sie so aus:

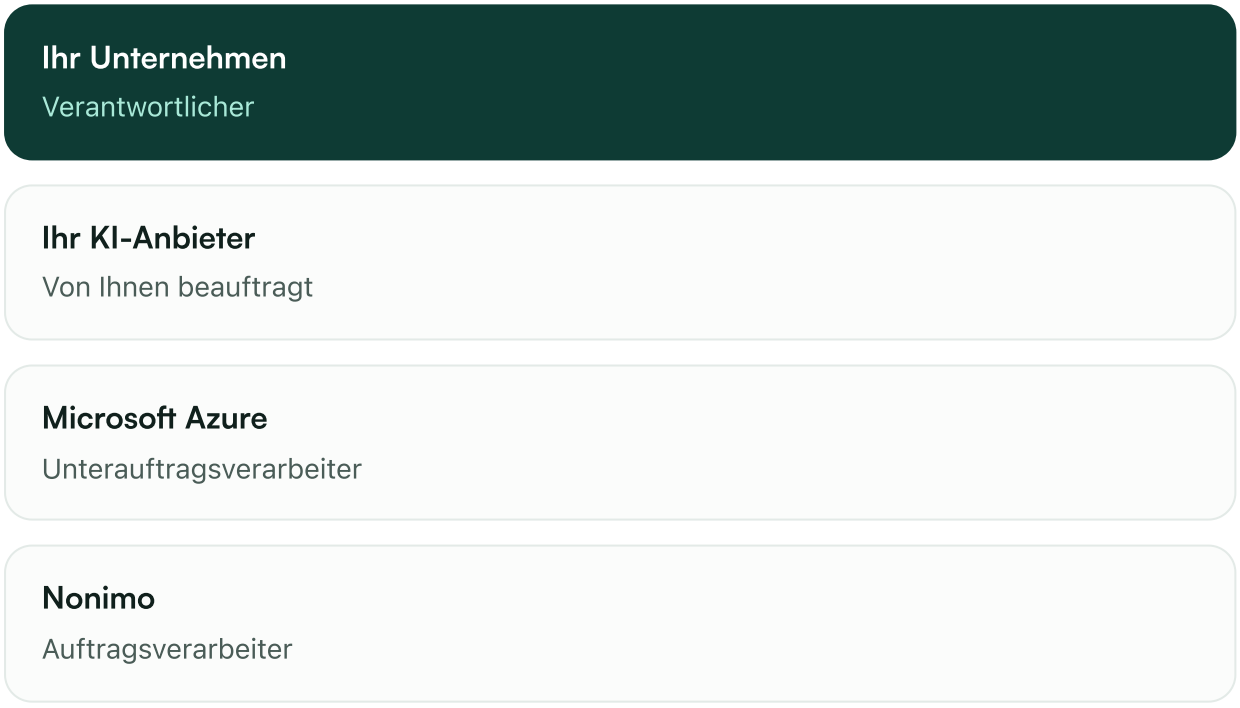

ABBILDUNG 3

Beteiligter	Rolle	Was er tut
Ihr Unternehmen	Verantwortlicher	Entscheidet über Zweck und Mittel, wählt den KI-Anbieter, legt die Einstellungen fest
Nonimo	Auftragsverarbeiter nach Art. 28 DSGVO	Verarbeitet den Text in Ihrem Auftrag auf Ihrer vertraulichen Maschine
Microsoft Azure	Unterauftragsverarbeiter	Stellt die vertrauliche Maschine in Irland bereit
Ihr KI-Anbieter	Von Ihnen mit eigenem Schlüssel beauftragt	Erhält die Anfrage mit Platzhaltern und liefert die Antwort
Cloudflare	Dienstleister außerhalb des Textwegs	Verwaltet Lizenzen und Zählerstände; am Text nicht beteiligt
Paddle	Autorisierter Händler (Merchant of Record), eigenständig verantwortlich für die Kaufdaten	Wickelt Kauf und Abrechnung ab

Der KI-Anbieter steht in Ihrem Vertragsverhältnis, nicht in unserem. Das hält die Kette übersichtlich: Ihr Vertrag mit dem Anbieter regelt dessen Verarbeitung, unser Vertrag mit Ihnen regelt die Verarbeitung im Gateway. Für Fragen zu Kauf und Rechnung ist Paddle Ihr Gegenüber; Informationen zu Tarifen finden Sie auf der Seite Preise.

07

Der rechtliche Rahmen in Deutschland

Die Bewertung im Einzelfall liegt bei Ihrem DSB. Nonimo Gateway gibt Ihnen für mehrere Vorschriften der DSGVO [1] eine konkrete technische und organisatorische Maßnahme an die Hand.

Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO. Personenbezogene Daten müssen auf das für den Zweck notwendige Maß beschränkt sein. Damit ein Sprachmodell ein Mahnschreiben formuliert, braucht es den Namen der Schuldnerin nicht. Platzhalter liefern dem Modell den Zusammenhang, die Identität erfährt es nicht.

Datenschutz durch Technikgestaltung, Art. 25 DSGVO. Der Verantwortliche soll geeignete Maßnahmen bereits bei der Gestaltung einer Verarbeitung treffen; Art. 25 nennt die Pseudonymisierung dabei ausdrücklich als Beispiel. Ein Gateway, das jede Anfrage zentral vorbereitet, setzt diesen Gedanken für alle angebundenen Anwendungen gleichzeitig um, statt ihn jeder Fachabteilung einzeln zu überlassen.

Sicherheit der Verarbeitung, Art. 32 Abs. 1 lit. a DSGVO. Die Vorschrift nennt Pseudonymisierung und Verschlüsselung als Maßnahmen zur Sicherheit. Nonimo Gateway liefert dazu passende Maßnahmen: Platzhalter auf dem Weg zum Anbieter, verschlüsselter Arbeitsspeicher auf der vertraulichen Maschine und verschlüsselte Speicherung der Einstellungen.

Auftragsverarbeitung, Art. 28 DSGVO. Nonimo verarbeitet die Texte in Ihrem Auftrag. Den Vertrag zur Auftragsverarbeitung schicken wir Ihnen auf Anfrage an hello@nonimo.ai.

Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO, und Datenschutz-Folgenabschätzung, Art. 35 DSGVO. Wenn Ihr Unternehmen KI-Dienste mit Kundendaten nutzt, gehört diese Verarbeitung ins VVT und oft in eine DSFA. Die Angaben dieses Whitepapers (Ort, Rollen, Speicherdauer, Maßnahmen) und die Nachweise aus dem nächsten Abschnitt fließen direkt in beide Dokumente ein.

Übermittlungen in Drittländer, Kapitel V DSGVO. Sitzt Ihr KI-Anbieter außerhalb der EU, prüfen Sie die Grundlage der Übermittlung wie bisher. Mit Nonimo Gateway enthält das, was die EU verlässt, statt der erkannten Namen, Konten und Ausweisnummern Platzhalter. Das geht unmittelbar in Ihre Risikobewertung der Übermittlung ein.

Pseudonymisierung als Rechtsbegriff

Juristisch ordnet man das Ersetzen identifizierender Werte durch Platzhalter als Pseudonymisierung im Sinne von Art. 4 Nr. 5 DSGVO ein. Für Ihr Unternehmen bleiben die Daten personenbezogen, und Sie behandeln sie auch so.

Der Europäische Datenschutzausschuss hat dazu im Januar 2025 die Leitlinien 01/2025 zur Pseudonymisierung angenommen und zur Konsultation gestellt [2]. Sie beschreiben, wie Pseudonymisierung als Schutzmaßnahme wirkt und wie sie in die Abwägung eingeht.

Erwägungsgrund 26 DSGVO stellt klar, dass anonyme Informationen nicht unter die Verordnung fallen. Wann Daten für einen Empfänger anonym sind, hat der Gerichtshof der Europäischen Union in seinem Urteil vom 4. September 2025 in der Rechtssache C-413/23 P (EDSB gegen SRB) präzisiert [3].

Pseudonymisierte Daten sind danach nicht zwangsläufig personenbezogen für einen Empfänger, der die betroffene Person nicht mit vernünftigerweise verfügbaren Mitteln reidentifizieren kann; maßgeblich ist die Sicht des jeweiligen Empfängers.

Wie weit das für Ihren konkreten KI-Anbieter trägt, bewertet Ihr DSB im Einzelfall. Für Ihre eigene Dokumentation behandeln Sie die Verarbeitung weiterhin als Verarbeitung personenbezogener Daten.

Die Orientierungshilfe der DSK

Die Datenschutzkonferenz des Bundes und der Länder hat am 6. Mai 2024 die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ veröffentlicht [4]. Sie richtet sich an Verantwortliche, die KI-Anwendungen auswählen und einsetzen, und ist für viele deutsche Datenschutzbeauftragte der erste Bezugspunkt.

Wer eine KI-Anwendung im Unternehmen einführt, findet in Nonimo Gateway eine Maßnahme, mit der sich die dort angesprochenen Fragen zu Datenminimierung, Transparenz der Verarbeitung und Rollen gut dokumentieren lassen.

08

Was als Nachweis bleibt

Als Nachweis liefert Nonimo Gateway zwei Arten von Unterlagen, beide im Dashboard und beide ohne einen einzigen personenbezogenen Wert.

Der Monatsbericht für den DSB. Er zeigt, wie viele personenbezogene Daten in einem Monat ersetzt wurden und welcher Art sie waren, ausschließlich als Zahlen. Ein fiktives Beispiel:

November	Ersetzte Daten
Personen	4.108
Unternehmen	1.256
Ausweis- und Steuernummern	1.874
Bankverbindungen (IBAN)	962
E-Mail-Adressen und Telefonnummern	1.117
Gesamt	**9.317**

Das Protokoll je Anfrage. Für jede Anfrage verzeichnet es Uhrzeit, KI-Anbieter, Modell und die Anzahl der ersetzten Daten je Art. Sie exportieren es als CSV oder JSONL. Das Protokoll enthält die Daten selbst nie, nur Zählwerte und Metadaten.

Wofür Ihr DSB diese Unterlagen nutzt:

- **Verzeichnis von Verarbeitungstätigkeiten:** Die Zahlen belegen, welche Datenkategorien in der Verarbeitung vorkommen und in welchem Umfang.
- **Datenschutz-Folgenabschätzung:** Der Bericht zeigt, dass die beschriebene Maßnahme im Betrieb greift, Monat für Monat.
- **Anfragen von Mandanten, Kunden oder Prüfern:** Sie können zeigen, wie viele Daten ersetzt wurden, ohne dabei selbst Daten herauszugeben.

> **Hinweis:** Weil Bericht und Protokoll nur Zahlen enthalten, können Sie sie an Revision, Wirtschaftsprüfer oder einen anfragenden Mandanten weitergeben, ohne vorher etwas schwärzen zu müssen.

09

Fragen, die Ihr DSB uns stellen kann

1. Wo werden unsere Texte verarbeitet? Auf einer vertraulichen Maschine von Microsoft Azure in Irland, die nur Ihrem Unternehmen dient.

2. Liest jemand bei Nonimo unsere Texte? Nein. Die Maschine startet nur veröffentlichte Versionen des Gateways, und was sie verarbeitet, wird von Mitarbeitenden von Nonimo und Microsoft nicht gelesen. Nonimo erhält ausschließlich Zahlen.

3. Welche Daten werden erkannt und ersetzt? Namen von Personen, Unternehmen, Ausweis- und Steuernummern, Bankverbindungen sowie E-Mail-Adressen und Telefonnummern. Dazu kommen die eigenen Begriffe, die Sie im Dashboard hinterlegen.

4. Bekommen unsere Mitarbeitenden die echten Namen in der Antwort zurück? Ja. Das Gateway setzt die echten Daten wieder ein, auch bei gestreamten Antworten und bei Tool Calls.

5. Was speichert das Gateway dauerhaft? Ihre Einstellungen, den Schlüssel Ihres KI-Anbieters und Ihre eigenen Begriffe, verschlüsselt und in derselben Region. Die Texte selbst werden nur durchgeleitet.

6. Wann wird alles gelöscht? Im Test nach drei Tagen in Folge ohne Nutzung (mit Hinweis einen Tag vorher), am Ende der Testphase ohne Tarif, am Ende des Abonnements oder auf Ihren Wunsch.

7. Welche Rolle hat Nonimo nach der DSGVO? Für die Texte, die über das gehostete Gateway laufen, ist Nonimo Auftragsverarbeiter; Ihr Unternehmen ist Verantwortlicher. Microsoft Azure ist Unterauftragsverarbeiter.

8. Wie erhalten wir den Vertrag zur Auftragsverarbeitung? Schreiben Sie an hello@nonimo.ai; wir senden ihn Ihnen zu.

9. Mit welchen KI-Anbietern funktioniert das? Mit dem KI-Anbieter, den Sie für Ihr Gateway wählen, etwa OpenAI oder Claude (Anthropic). Sie nutzen Ihren eigenen Vertrag und Ihren eigenen Schlüssel.

10. Was müssen wir in unseren Anwendungen ändern? Die Zieladresse und den Schlüssel, meist zwei Zeilen. SDK, Modelle und Programmlogik bleiben unverändert, auf Ihren Servern wird nichts installiert.

11. Was bekommen wir für VVT und DSFA? Einen Monatsbericht mit den ersetzten Daten nach Art und ein Protokoll je Anfrage als CSV oder JSONL, beide nur mit Zahlen.

12. Wer ist für Kauf und Rechnung zuständig? Paddle, als autorisierter Händler (Merchant of Record) und eigenständig Verantwortlicher für die Kaufdaten.

Weitere Angaben zum Schutzkonzept finden Sie auf unserer Seite Sicherheit, einen Überblick über das Produkt auf der Startseite.

10

Quellen

1. Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), Art. 4 Nr. 5, Art. 5 Abs. 1 lit. c, Art. 25, 28, 30, 32 Abs. 1 lit. a, 35, Kapitel V, Erwägungsgrund 26: https://eur-lex.europa.eu/eli/reg/2016/679/oj
2. Europäischer Datenschutzausschuss (EDSA), Leitlinien 01/2025 zur Pseudonymisierung, angenommen am 16. Januar 2025 (öffentliche Konsultation): https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en
3. Gerichtshof der Europäischen Union, Urteil vom 4. September 2025, Rechtssache C-413/23 P, EDSB gegen SRB: https://curia.europa.eu/juris/liste.jsf?num=C-413/23
4. Datenschutzkonferenz (DSK), Orientierungshilfe „Künstliche Intelligenz und Datenschutz“, 6. Mai 2024: https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf
5. Microsoft, Dokumentation zu Azure Confidential Computing: https://learn.microsoft.com/azure/confidential-computing/