MadeForPrivacy

RELEASE-DOKUMENT

Datenschutz- und Betriebskonzept

Wie MadeForPrivacy in deiner Umgebung läuft, welche Daten wo liegen, wer sie sieht und welche Maßnahmen das absichern. Für Datenschutzbeauftragte, IT und Geschäftsführung, die über einen datenschutzkonformen Betrieb entscheiden.

STAND	19.10.2026
SYSTEM	MadeForPrivacy (Server-Stack, Desktop- und Web-Client)
BETREIBER	Kunde, in kundeneigener Infrastruktur oder eigener Cloud
SOFTWAREANBIETER	NeckarByte UG (haftungsbeschränkt), Ludwigsburg
GELTUNGSBEREICH	Server-Stack (Docker Compose), Desktop-Client für Windows und Web-Client, konfigurierte KI-Dienste je Datenzone, Knowledge (RAGFlow), Webrecherche (SearXNG), Jobs, Mailbox und Item-Relay, Handbücher

Inhalt

0	Kernaussagen	3
1	Rollen und Verantwortlichkeiten	3
2	Architektur und Datenflüsse	4
3	Datenklassen	7
4	Datenzonen und Unterauftragsverarbeiter je Zone	9
5	Speicherung, Verschlüsselung, Aufbewahrung und Löschung	12
6	Zugriff und Rechte	15
7	Protokollierung	16
8	Schutz vor Prompt Injection	17
9	Betroffenenrechte	18
10	Technische und organisatorische Maßnahmen	19
11	Restrisiken	20
12	Kontakt und Pflege des Dokuments	21
A	Anhang: Einstellungen mit Datenschutzbezug	21

0 Kernaussagen

- **Du betreibst, du bist verantwortlich.** MadeForPrivacy läuft als Docker-Compose-Stack auf deinem Server oder in deiner Cloud. NeckarByte hat im Standardbetrieb keinen Zugriff auf deine Instanz und ist dann kein Auftragsverarbeiter.
- **Datenzonen sind Technik, nicht Absicht.** Jeder Agent, jedes Tool und jeder KI-Dienst trägt eine der Zonen 🟣 **Nur lokal**, 🟢 **DSGVO-konform** oder 🔴 **Ungeschützt**. Ein Agent darf nur Dienste seiner eigenen oder einer strengeren Zone aufrufen; passt kein Dienst, läuft der Schritt nicht.
- **Der Server hält keine Gespräche.** Konversationen liegen im Client (Desktop: verschlüsselter Vault pro Benutzer). Große Nutzdaten zwischen Client, Server und Workern liegen AES-256-GCM-verschlüsselt mit Ablaufzeit (Standard 24 Stunden) im Item-Relay.
- **Persistent sind Metadaten und bewusst angelegte Wissensbestände:** Benutzerprofile, Konfiguration, Änderungshistorie, Ausführungsverfolgung (wer, welcher Agent, welcher Dienst, Tokens, Kosten), Knowledge-Datasets und Gedächtnisse, Handbücher.
- **Zonen ersetzen keine Verträge.** Auftragsverarbeitungsverträge mit KI-Anbietern, Rechtsgrundlagen, Lösch- und Aufbewahrungsfristen bleiben Sache deiner Organisation. Dieses Dokument liefert die technischen Fakten dafür.

Begriffe: Die Plattform arbeitet *datenschutzkonform*; „DSGVO-konform" ist der Name der mittleren Datenzone, so wie sie im Client erscheint. „Neva" ist die persönliche Assistentin der Plattform. „Aktenkoffer" (Briefcase) ist der typisierte Datencontainer eines Agentenlaufs.

1 Rollen und Verantwortlichkeiten

Die Instanz gehört dir. Alles, was in ihr verarbeitet wird, verarbeitest du als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. NeckarByte liefert Software, Updates und nach Vereinbarung Einrichtung und Support.

PARTEI	ROLLE	ZUGRIFF AUF DEINE DATEN	VERTRAGLICHE EINORDNUNG
Du (Kunde)	Betreiber der Instanz, legt Zonen, Dienste, Agenten, Gruppen und Fristen fest	vollständig	Verantwortlicher
NeckarByte UG	Softwareanbieter und Lizenzgeber; Updates und Ticket-Support im Grundsupport	keiner im Standardbetrieb	kein Auftragsverarbeiter, solange kein Zugriff besteht

PARTEI	ROLLE	ZUGRIFF AUF DEINE DATEN	VERTRAGLICHE EINORDNUNG
NeckarByte UG als Betreiberpartner	Einrichtung, Konfiguration, Fehleranalyse, Agentenpflege auf deiner Instanz, nur nach Vereinbarung und je Vorgang	in einer Fernwartungssitzung, die du startest und freigibst: was auf dem freigegebenen Bildschirm zu sehen ist, mit den Rechten deines angemeldeten Admins (Abschnitt 6.3)	Auftragsverarbeitung nach Art. 28 DSGVO: Der AVV von NeckarByte deckt Fernwartung und Support ab. Das Muster schicken wir dir auf Anfrage vor dem ersten Supportfall.
KI-Anbieter (z. B. Microsoft Azure)	Inferenz für Dienste, die du in den Zonen DSGVO-konform oder Ungeschützt freigibst	Prompt-Daten des jeweiligen Schritts	dein Auftragsverarbeiter; Vertrag und Region wählst du direkt beim Anbieter
Betreiber externer Suchmaschinen	Treffer für die Webrecherche über deine SearXNG-Instanz	nur freigegebene, neutralisierte Suchbegriffe	Empfänger ohne Personenbezug im Regelfall; siehe Abschnitt 4
Deine Fachsysteme	Postfächer, Datenbanken, REST-APIs, Netzlaufwerke, SharePoint/OneDrive über den Sync-Dienst	wie von dir angebunden	in deinem Verantwortungsbereich, bestehende Verträge gelten weiter

Der Standardbetrieb ohne Zugriff ist technisch der Normalfall: Die Instanz ruft keine Server von NeckarByte auf, um zu funktionieren. Updates kommen als Container-Images aus einer Registry, die du ziehst; die Lizenz ist eine signierte Datei in deinem Datenordner und wird ohne Verbindung nach außen geprüft. Die Instanz sendet keine Telemetrie und keine Fehlerberichte; der Desktop-Client sucht Updates nur bei deinem eigenen Server.

2 Architektur und Datenflüsse

Ein Stack aus Containern auf einem Server, der Client auf dem Arbeitsplatz, externe Dienste nur

dort, wo du sie konfigurierst.

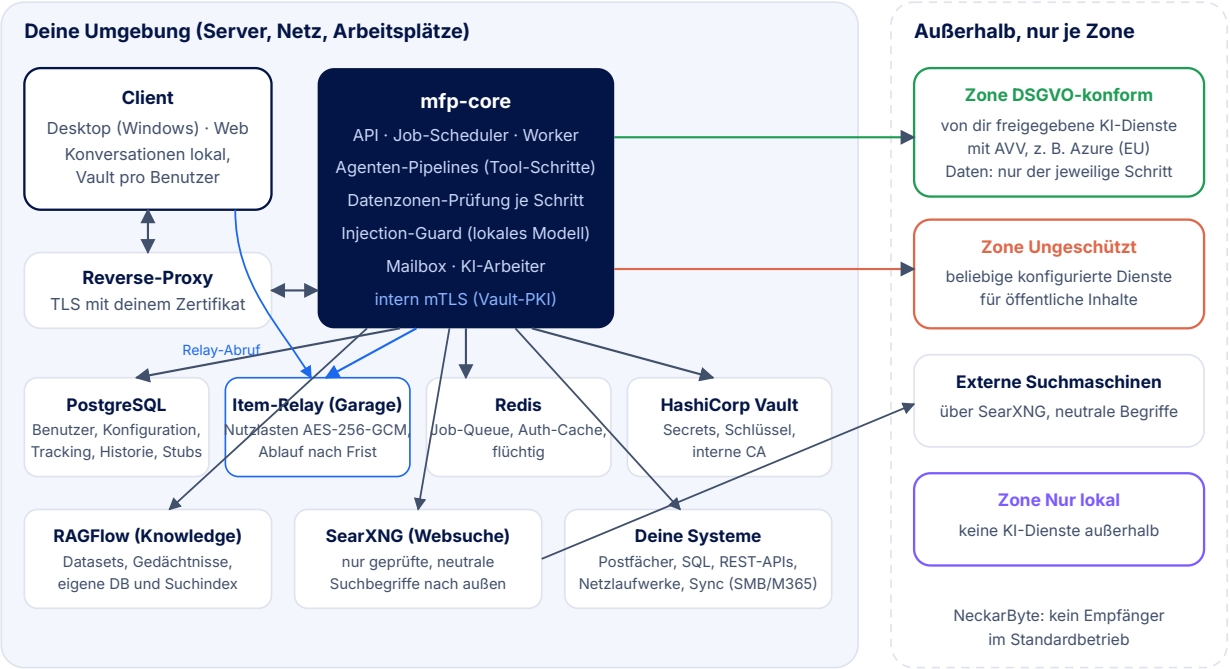

Abbildung 1: Komponenten und Datenflüsse. Innerhalb deiner Umgebung sprechen die Dienste über mTLS; nach außen geht nur, was die Datenzone des jeweiligen Schritts erlaubt.

2.1 Bausteine

BAUSTEIN	AUFGABE	PERSISTENTE INHALTE
Client	Desktop-App für Windows (signierter MSI-Installer, Selbst-Update über deinen Server) oder Web-Build im Browser; Konversationen, Anzeige, Anhänge	Desktop: ja, im verschlüsselten Vault pro Benutzer. Web: Browser-Speicher
mfp-reverseproxy	TLS-Endpunkt mit deinem Zertifikat, Routing zu Core, Frontend, Docs	nein
mfp-core	API, Job-Scheduler und Worker-Prozesse; führt Agenten-Pipelines Schritt für Schritt aus, prüft Zonen, verfolgt Ausführungen	nein (Laufzeit im Arbeitsspeicher der Worker)
mfp-database (PostgreSQL)	Benutzer und Profile, Gruppen, Konfiguration (Agenten, Tools, KI-Dienste, Anmeldeanbieter), Änderungshistorie, Ausführungsverfolgung, Feedback, Job- und Mailbox-Zeilen (nur Verweise)	ja
mfp-relay-store (Garage, S3-kompatibel)	Item-Relay: große Aktenkoffer-Nutzlasten und Zustellungen, verschlüsselt, mit Ablaufzeit	temporär
mfp-cache (Redis)	Job-Queue und Ereignisse, Anmelde-Cache, optionaler Tool-Cache (z. B. abgerufene Webseiten mit TTL)	flüchtig

BAUSTEIN	AUFGABE	PERSISTENTE INHALTE
mfp-vault (HashiCorp Vault)	Secrets (Zugangsdaten, API-Schlüssel, Relay-Schlüssel) als `secret::`-Referenzen, interne PKI für mTLS	ja (Secrets)
RAGFlow-Stack	Knowledge: Datasets (Dokumentenindex) und Gedächtnisse, hybride Suche; eigene Datenbank, Suchindex, Objektspeicher	ja, bewusst befüllt
mfp-sync	Dateisynchronisation für Knowledge aus SMB, OneDrive, SharePoint, lokalen Ordnern	Arbeitskopien der freigegebenen Quellen
mfp-websearch (SearXNG)	Webrecherche über eine eigene Suchinstanz	nein
mfp-docs, mfp-frontend	Produktdokumentation und Web-Oberfläche	nein

2.2 Ablauf eines Agentenlaufs

1. Der Benutzer sendet im Client eine Nachricht mit Aktenkoffer (Text, Dateien, frühere Items). Große Items reisen als Verweis (`relay_download_id`), wenn der Server sie schon kennt.
2. Die API lagert große Items ins Item-Relay aus, legt einen Job in der Datenbank an (mit Verweisen, nicht mit Inhalten) und reiht ihn in Redis ein. Jobs laufen nie im API-Prozess.
3. Ein Worker übernimmt den Job, löst die Verweise auf und führt die Pipeline aus. Jeder Tool-Schritt sieht nur die Items seiner konfigurierten Eingabetypen; ein KI-Aufruf bekommt den Ausschnitt, den der Schritt braucht, nicht den ganzen Aktenkoffer.
4. Vor jedem KI-Aufruf wird die Zone geprüft: nur Dienste der Agentenzone oder einer strengeren. Jeder Aufruf wird mit Dienst, Schritt, Tokens, Kosten, Dauer und Zone in der Ausführungsverfolgung erfasst.
5. Das Ergebnis wird an den Client gestreamt; große Items wieder als Relay-Verweis, den der Client bei Bedarf lädt. Der Client speichert die Unterhaltung lokal.

Weitere Wege mit derselben Technik: **Mailbox** (ein Agent stellt eine Nachricht oder ein Signal an andere Benutzer zu; die Datenbank hält nur Verweise, die Nutzlast liegt im Relay mit derselben Ablaufzeit wie die Zeile), **KI-Arbeiter** (überwachen z. B. ein Postfach oder einen Ordner und starten je Fund einen Job) und **Subcalls** (Neva beauftragt einen Spezialisten-Agenten mit genau den Items, die der Schritt braucht).

3 Datenklassen

Welche Daten die Plattform anfasst, wo sie liegen und ob sie Personenbezug haben können.

DATENKLASSE	BEISPIELE	ORT	DAUER	PERSONEN-BEZUG
Konversationen	Nachrichten, Antworten, angehängte Items	Client (Desktop-Vault pro Benutzer, Web: Browser)	bis zur Löschung; in den Zonen Nur lokal und DSGVO-konform zentral begrenzt (`retention.client_message_days`, Standard 365 Tage); in der Zone Ungeschützt keine zentrale Frist	ja
Laufzeitdaten	Aktenkoffer eines Laufs, Zwischenergebnisse, Prompt-Kontext	Arbeitsspeicher des Workers	Dauer des Laufs	ja
Relay-Nutzlasten	Dokumenttexte, Bilder, Mail-Bodies, Zustellungen	Item-Relay (Garage), AES-256-GCM	`retention.relay_hours`, Standard 24 h; Sweep alle 5 Minuten	ja
Uploads und E-Mails	PDF, DOCX, XLSX, Bilder, EML/MSG inkl. Anhängen; bei aktivem `preserve_html_body` auch der HTML-Teil der Mail	Aktenkoffer, Relay; dauerhaft nur, wenn ein Schritt bewusst in Knowledge, ein Handbuch oder ein Zielsystem schreibt	wie Laufzeit/Relay	ja
Benutzerprofile	Benutzername, Anzeigename, Vor- und Nachname, E-Mail, Abteilung, Gruppen (aus dem Verzeichnis oder manuell), Anmeldeanbieter, Zeitpunkt der letzten Nutzung des Zugangsschlüssels (in der Benutzerverwaltung als „Zuletzt gesehen“ und als „Online“, wenn er in den letzten 5 Minuten genutzt wurde). Telefon, Mobilnummer, Funktion, Firma und Porträt speichert der Server nicht	Datenbank	bis zur Löschung des Benutzers	ja

DATENKLASSE	BEISPIELE	ORT	DAUER	PERSONEN-BEZUG
Porträts	Profilbild aus dem Verzeichnis (AD, LDAP, Microsoft Graph), wenn das Attribut gemappt ist; bei der Anmeldung gelesen, auf höchstens 256 px verkleinert und als JPEG neu geschrieben	nur im Client (verschlüsselter lokaler Speicher); der Server reicht das Bild in der Anmeldeantwort durch und speichert es weder in der Datenbank noch im Blob-Store	wie die lokalen Daten des Clients	ja (biometrienah, aber kein biometrisches Template)
Ausführungsverfolgung	Agentenlauf, Tool-Schritt, KI-Anfrage: Benutzername, Abteilung, Agent, Dienst, Modell, Tokens, Kosten, Dauer, Status, Zone; dazu **Inhaltsfelder**: Fehlertexte und, nur bei Agenten im Debug-Modus, Aktenkoffer-Vorschauen	Datenbank	Inhaltsfelder bis `retention.debug_content_days` (Standard 30 Tage); Benutzername bis `retention.username_months` (Standard 13 Monate), danach bleibt die Nutzung nur der Abteilung zugeordnet; Metadaten bis `retention.metadata_months` (Standard 0 = dauerhaft)	ja (Benutzername; Vorschauen können Inhalte tragen)
Nutzung und Limits	Aggregate je Tag, Dienst, Benutzer; Kostenlimits je Gruppe	abgeleitet aus der Ausführungsverfolgung	wie oben	ja (pro Benutzer)
Änderungshistorie	Wer hat wann in welchem Bereich was angelegt, geändert, gelöscht, mit altem und neuem Wert (Geheimnisse maskiert); abgeschlossene Änderungssätze der Freigabe-Warteschlange	Datenbank	`retention.audit_log_months`, Standard 60 Monate	ja (Admin-Identität)
Feedback	Bewertung und Kommentar des Benutzers mit der gespeicherten Nachricht und dem Prompt	Datenbank	`retention.feedback_days`, Standard 365 Tage	ja
Anwendungslogs	Serverlogs je Tag, Live-Log im Status	Logverzeichnis	`retention.log_days`, Standard 28 Tage	möglich

DATENKLASSE	BEISPIELE	ORT	DAUER	PERSONEN-BEZUG
Knowledge	Datasets (Dokumente aus Freigaben, Uploads), Gedächtnisse (z. B. Nevas Gedächtnis je Benutzer: Fakten, die die Person über sich sagt)	RAGFlow	bis zur Löschung durch Admin, Agent oder Benutzer, oder bis das Dokument aus der Quelle verschwindet; keine zeitbasierte Frist	möglich bis ja
Handbücher	Markdown-Dokumente in git-Arbeitsbäumen, inkl. persönlichem Handbuch je Benutzer	Handbücher-Wurzel auf dem Server (git)	Commit-Historie bleibt	möglich
Konfiguration	Agenten, Tools, KI-Dienste, Anmeldeanbieter, Gruppen-Mappings, Fristen	Datenbank, Datenordner	dauerhaft	gering
Secrets	Zugangsdaten, API-Schlüssel, Relay-Schlüssel, Zertifikate	Vault; in der Konfiguration nur Referenzen	dauerhaft, rotierbar	indirekt
Berichte	Von Agenten erzeugte Dateien	Netzwerkpfad (UNC) oder lokaler Ordner nach Konfiguration	deine Richtlinie	möglich
Backups	Datenbank-Dump, Datenordner (Core, Relay, RAGFlow, Vault, Zertifikate), `.env`	dein Backup-Ziel	`MFP_BACKUP_RETENTION_DAYS`, Standard 14 Tage	ja

4 Datenzonen und Unterauftragsverarbeiter je Zone

Die Zone entscheidet, welche Dienste ein Schritt aufrufen darf. Daraus folgt, wer außerhalb deiner Umgebung Daten sehen kann und wer nicht.

ZONE	GEDACHT FÜR	WAS DER BENUTZER ERWARTEN DARF	ZULÄSSIGE DIENSTE
Nur lokal	interne Dokumente, Mitarbeiterdaten, Verträge	Inferenz nur im eigenen Haus; kein Suchbegriff geht nach außen. Einzige Verbindung nach außen: Webseiten, deren Adresse der Benutzer selbst nennt (4.1)	nur Dienste mit Zone Nur lokal
DSGVO-konform	Kundendaten, Auftragsdaten, Korrespondenz	Verarbeitung nur über Dienste, die du dafür freigegeben hast, datensparsam und protokolliert	Nur lokal oder DSGVO-konform

ZONE	GEDACHT FÜR	WAS DER BENUTZER ERWARTEN DARF	ZULÄSSIGE DIENSTE
Ungeschützt	öffentliche oder wenig sensible Inhalte: Marketing, Entwürfe, öffentliche Recherche	Daten können von externen Diensten verarbeitet werden; der Client zeigt dazu ein eigenes Kennzeichen	alle konfigurierten Dienste

Die Regel wird im Server erzwungen, nicht nur angezeigt: Passt zu einem Schritt kein Dienst der erlaubten Zonen, schlägt die Ausführung fehl, statt Daten in eine offenere Zone zu schicken. Bei Neva und der dynamischen Agentenauswahl wählt der Benutzer die Zone per Kennzeichen; sie filtert, welche Spezialisten überhaupt in Frage kommen. Jede KI-Anfrage trägt in der Ausführungsverfolgung, ob sie in der Zone DSGVO-konform lief.

4.1 Empfänger außerhalb deiner Umgebung je Zone

ZONE	EMPFÄNGER	DATEN	VERTRAGLICHE GRUNDLAGE
Nur lokal	keine. Lokale Modelle (z. B. Ollama, ein lokaler OpenAI-kompatibler Endpunkt, ComfyUI) laufen in deiner Umgebung	–	keine zusätzliche nötig
DSGVO-konform	die KI-Dienste, die du dieser Zone zuweist, typisch Microsoft Azure (Azure OpenAI oder Azure AI Services) in einer EU-Region, mit den Datenschutzbedingungen von Microsoft	Prompt und Antwort des jeweiligen Schritts; keine Konten, keine Schlüssel, kein ganzer Aktenkoffer	dein Vertrag mit dem Anbieter (AVV, Region, keine Nutzung zum Training). Welche Dienste, Regionen und Verträge in deiner Instanz gelten, steht in der Anlage „KI-Dienste deiner Instanz", die NeckarByte je Kunde liefert.
Ungeschützt	beliebige konfigurierte Anbieter: OpenAI-kompatible APIs, Hugging-Face-Endpunkte, Bild-Dienste	Prompt und Antwort des Schritts	deine Entscheidung; nur für Inhalte ohne Personenbezug

ZONE	EMPFÄNGER	DATEN	VERTRAGLICHE GRUNDLAGE
Webrecherche (alle Zonen mit Websuche)	Betreiber der Suchmaschinen, die deine SearXNG-Instanz abfragt; danach die abgerufenen Webseiten	In der Zone DSGVO-konform nur Suchbegriffe, die ein zweistufiger Filter (deterministisch, dann KI-Prüfung) als neutral freigegeben hat; die ursprüngliche Eingabe geht nie nach außen. Aus Adressen, die der Benutzer nennt, entfernt das Tool Kennungen oder verwirft die Adresse. In der Zone Nur lokal sucht das Tool nicht: Der Agent antwortet mit den Suchbegriffen, die er verwendet hätte, als Text. Adressen, die der Benutzer ausdrücklich nennt, ruft das Tool auch in Nur lokal ab; der Betreiber der Seite sieht dabei die IP-Adresse deines Servers.	keine Auftragsverarbeitung, da ohne Personenbezug; Restrisiko siehe Abschnitt 11
Knowledge-Sync	Microsoft 365 (OneDrive, SharePoint), wenn du diese Quellen anbindest	Lesezugriff auf freigegebene Ordner	dein bestehender Vertrag mit Microsoft
Alle Zonen	NeckarByte	keine	kein Empfänger im Standardbetrieb

Anbietertypen im Produkt: `azure`, `openai` (OpenAI-kompatibel), `ollama`, `local`, `huggingface`, `azure_bfl` (Bild), ComfyUI. Jeder konfigurierte Dienst trägt genau eine Zone, Zugangsdaten als Vault-Referenz, Ratenlimits und Preise je Million Tokens für die Kostenschätzung. Welche Dienste in welcher Zone stehen, legst du bei der Einrichtung fest; der Vorschlag von NeckarByte lautet: lokale Modelle für Nur lokal, ein EU-Azure-Dienst für DSGVO-konform, nichts in Ungeschützt, bis es einen Bedarf gibt. Die konkrete Liste deiner Instanz (Dienst, Zone, Region, Vertragsreferenz) ist nicht Teil dieses Dokuments, weil sie je Kunde verschieden ist und sich mit jeder Modellwahl ändert; du bekommst sie als eigene Anlage.

5 Speicherung, Verschlüsselung, Aufbewahrung und Löschung

Je Speicherort: wie verschlüsselt, wie lange, wie gelöscht, was du einstellen kannst.

SPEICHER-ORT	VERSCHLÜSSELUNG	AUFBEWAHRUNG	LÖSCHUNG	EINSTELL-BAR
Desktop-Client	Vault pro Benutzer, eine verschlüsselte Datei je Eintrag; Schlüssel über Electron safeStorage (Windows: DPAPI). Der Renderer läuft in einer In-Memory-Sitzung: kein unverschlüsselter Browser-Speicher auf der Festplatte, auch nicht für einen zweiten Windows-Benutzer	Nachrichten der Zonen Nur lokal und DSGVO-konform entfernt der Client nach `retention.client_message_days` (Standard 365). Für die Zone Ungeschützt, die nur für Inhalte ohne Personenbezug gedacht ist, gilt keine zentrale Frist; diese Unterhaltungen löscht der Benutzer selbst.	durch den Benutzer (Unterhaltung löschen) und zentral per Frist	ja (Server-Einstellung)
Web-Client	Browser-Speicher, Vertrauensgrenze ist der Browser; keine Trennung pro Benutzer in einem geteilten Profil	wie Desktop-Frist	durch den Benutzer, Browserdaten	–
Item-Relay (Garage)	AES-256-GCM, Schlüssel und HMAC-Geheimnis im Vault; Objekt-ID ist ein HMAC über den Inhalt	`retention.relay_hours`, Standard 24 h; eine Mailbox-Nachricht kann eine eigene Lebensdauer verlangen	Sweep alle `relay.sweep_interval_seconds` (Standard 300 s) löscht abgelaufene Objekte und Mailbox-Zeilen	ja
PostgreSQL	Transport mTLS über die interne CA; Verschlüsselung des Datenträgers ist Sache deiner Infrastruktur	Profile und Konfiguration dauerhaft; Ausführungsverfolgung, Änderungshistorie, Feedback und Jobzeilen nach ihren Fristen (Anhang)	Benutzer löschen (Admin); periodische Löschläufe: Inhaltsfelder der Verfolgung auf NULL, freie Metadaten auf Zahlen und Flags reduziert, Benutzernamen entfernt, abgeschlossene Jobzeilen nach `retention.job_days` (Standard 30 Tage), Feedback und Änderungshistorie nach ihren Fristen	ja
Redis	Transport mTLS; nur flüchtige Daten	TTL je Eintrag (Auth-Cache, Tool-Cache `tool_cache_ttl_seconds`)	automatisch	ja

SPEICHERORT	VERSCHLÜSSELUNG	AUFBEWAHRUNG	LÖSCHUNG	EINSTELLBAR
Anwendungslogs	Dateisystem des Servers	`retention.log_days`, Standard 28 Tage	Sweep löscht ganze Tagesverzeichnisse	ja (0 = unbegrenzt)
RAGFlow	eigene Datenbank, Index und Objektspeicher im Stack; Datenträger-Verschlüsselung Sache der Infrastruktur	bis zur Löschung; keine zeitbasierte Frist, weil Wissen eine eigene Quelle mit eigenem Lebenszyklus hat	Admin (Knowledge: einzelne Dokumente und Gedächtniseinträge oder die ganze Quelle), Lösch-Tool in Pipelines, Benutzer bei `user_deletable`-Gedächtnissen; der Sync entfernt Dokumente, die aus der angebundenen Quelle verschwinden	teilweise
Handbücher (git)	Dateisystem des Servers; optionales Remote mit Token aus dem Vault	Historie bleibt	Löschen ist ein neuer Commit, frühere Fassungen bleiben in der Historie. Eine Funktion zum Entfernen aus der Historie gibt es nicht. Handbücher sind für Abläufe gedacht, nicht für personenbezogene Vorgänge; stehen doch welche darin, legt dein Admin das Handbuch auf Anfrage neu an (Restrisiko, Abschnitt 11)	–
Vault	Vault-eigene Verschlüsselung, Unseal-Schlüssel beim Betreiber	dauerhaft	Rotation und Löschung über Vault	ja
Server-Backups	`backup-stack.sh` erzeugt DB-Dump, komprimierte Archive, Prüfsummen und eine Kopie der `.env`; das Skript verschlüsselt nicht, der Backup-Speicher muss also geschützt sein. Relay-Blobs und Vault-Daten sind darin weiterhin verschlüsselt	`MFP_BACKUP_RETENTION_DAYS`, Standard 14	Retention des Skripts; gelöschte Daten können bis zum Ablauf in Backups liegen	ja

SPEICHERORT	VERSCHLÜSSELUNG	AUFBEWAHRUNG	LÖSCHUNG	EINSTELLBAR
Client-Backups	Die Sicherung des Clients (Einstellungen → Backup) verschlüsselt jedes Archiv mit AES-256-GCM unter einem frischen Datenschlüssel. Den Datenschlüssel bindet der Client an einen öffentlichen Schlüssel (ECDH, P-256); der private Schlüssel liegt nur beim Benutzer. Der Client kann Sicherungen schreiben, aber nicht selbst lesen; nur die Wiederherstellung braucht den privaten Schlüssel	Standard: die letzten 10 Archive; Anzahl und Höchstalter stellst du im Client ein	durch den Benutzer, indem er die Archive löscht	ja (Client)
Berichte, Zielsysteme	deine Freigaben und Systeme	deine Richtlinie	deine Prozesse	–

5.1 Transport und interne Kommunikation

- Client zu Server: TLS am Reverse-Proxy mit deinem Zertifikat (im Test selbst signiert).
- Zwischen den Containern (Core, Frontend, Datenbank, Cache, Reverse-Proxy): mTLS mit Zertifikaten aus der internen CA in Vault (`vault-pki-bootstrap`, `vault-pki-issue`, Erneuerung per Skript).
- Zu KI-Diensten und Fachsystemen: HTTPS; Zugangsdaten werden erst zur Laufzeit aus dem Vault aufgelöst und erscheinen weder in Konfigurationsexporten noch in der Oberfläche (maskiert).

5.2 Löschkonzept in Kürze

ANLASS	WAS PASSIERT
Mitarbeiter verlässt das Unternehmen	Konto an der Identitätsquelle deaktivieren, Gruppen entziehen, Benutzer in MFP löschen: Das entfernt Konto, Sitzungen, Mailbox-Zeilen und Bereichsrechte sofort. Der Name in den Nutzungsdaten verschwindet nach 13 Monaten oder sofort über „Benutzer aus Nutzungsdaten entfernen"; im Änderungsprotokoll bleibt er als Nachweis bis zur Frist. Zwei Schritte macht der Admin von Hand, weil das Benutzerlöschen sie nicht mit erledigt: in Knowledge die benutzerbezogenen Bestände der Person löschen (je benutzerbasierter Quelle ein eigener Bestand, am Namen mit der Benutzer-ID erkennbar, zum Beispiel Nevas Gedächtnis) und den Ordner ihres persönlichen Handbuchs auf dem Server löschen. Lokale Daten auf dem Arbeitsplatz: Benutzerprofil des Rechners.
Einzelne Unterhaltung	Benutzer löscht sie im Client. Serverseitig existiert sie nicht; Relay-Objekte laufen ab.
Dokument aus Knowledge entfernen	Admin oder Lösch-Tool entfernt es im Dataset; Chunks und Index werden entfernt. Backups halten es bis zum Ablauf der Backup-Retention.
Betroffenenanfrage „alles löschen"	Kombination aus Benutzerlöschung, „Benutzer aus Nutzungsdaten entfernen", Löschen der benutzerbezogenen Knowledge-Bestände, Knowledge-Suche nach der Person, Handbuch-Commit (bei Bedarf Neuanlage des Handbuchs); Inhaltsfelder der Verfolgung laufen nach 30 Tagen aus, Logs nach 28 Tagen.

6 Zugriff und Rechte

Anmeldung über dein Verzeichnis, Rechte über deine Gruppen. Nichts wird pro Person frei vergeben.

6.1 Anmeldung

ANBIETER	WOFÜR	PROFILDATEN, DIE ÜBERNOMMEN WERDEN
LDAP	Anmeldung und Benutzersuche gegen dein Verzeichnis; Bind-Passwort als Vault-Referenz	Benutzername (kanonisch aus dem Verzeichnis), Anzeigename, E-Mail, Gruppen, optional Porträt-Attribut
Kerberos Active Directory	Single Sign-on mit Windows-Anmeldung (Keytab, SPN)	wie LDAP
OAuth (Microsoft Entra ID)	ID-Token-Prüfung über JWKS, Gruppen und Porträt aus Microsoft Graph (`User.Read`)	Identität, Gruppen, Porträt
Lokale Benutzer	vom Admin angelegt, Passwort als bcrypt-Hash, vom Benutzer änderbar	nur, was der Admin pflegt
Config-API-Schlüssel, feste API-Schlüssel	Bootstrap und System-zu-System-Zugriffe mit Gruppenrechten; einmalige Anzeige, Rotation, Widerruf	–
Demo	nur Demonstrationen und Piloten, nie produktiv	–

Nicht vorhanden: RADIUS und andere OAuth-Anbieter als Entra ID (z. B. Google). Konten sind an den Anbietertyp gebunden, der sie angelegt hat; ein anderer Anbieter kann ein bestehendes Konto nicht übernehmen. Fehlgeschlagene Passwort-Anmeldungen werden je Benutzername und Adresse gedrosselt (HTTP 429), bevor ein Anbieter gefragt wird.

6.2 Rechte

OBJEKT	STEUERUNG
Agenten	sichtbar und ausführbar nur für die konfigurierten Gruppen (`ad_groups`); Erweiterter Modus je Agent zusätzlich über `enhanced_ad_groups`
Knowledge-Quellen	Zugriffsgruppen je Quelle; zur Laufzeit nutzen Tools nur Quellen, die der aktuelle Benutzer verwenden darf; benutzerbasierte Quellen trennen je Benutzer, Abruf und Ablage filtern nach Benutzer und Agent
Handbücher	Lese- und Schreibgruppen je Handbuch; leere Leseliste sperrt jeden Nicht-Admin; persönliches Handbuch nur für die Eigentümerin oder den Eigentümer, ohne Admin-Bypass

OBJEKT	STEUERUNG
Einstellungsbereiche	Bereichsberechtigungen je Gruppe oder Benutzer (Server, Agenten, Tools, KI-Dienste, Knowledge, Anmeldeanbieter, Benutzer, API-Schlüssel, Vorlagen, Lizenz, Feedback, Status, Nutzung); volle Admins über die Verzeichnisgruppe
Kosten	optionale rollierende Kostenlimits je Gruppe (Tag, Arbeitswoche, Monat) und ein Parallel-Limit je Benutzer
Mailbox	nur Agenten stellen zu, an konfigurierte Benutzer oder Gruppen; Benutzer lesen nur eigene Zeilen; Relay-Objekte sind an die erlaubten Benutzer-IDs gebunden
Serverseitige Identität	das `user`-Item eines Laufs setzt der Server; ein vom Client gesendetes wird verworfen. Ebenso baut der Server den Subcall-Kontext selbst; Bedingungen darauf können Arbeit nur einschränken, nie Zugriff gewähren

6.3 Supportzugriff von NeckarByte

Support läuft über Tickets. Braucht ein Fall einen Blick auf deine Instanz, nutzt NeckarByte eine Fernwartungssitzung mit RustDesk über einen selbst betriebenen RustDesk-Server. NeckarByte hat kein eigenes Konto in deiner MFP-Instanz und keinen ständigen Zugang.

- Du startest die Sitzung und gibst sie frei. Der Techniker arbeitet im Client mit dem Konto deines angemeldeten Admins, das heißt mit genau dessen Rechten. Die Sitzung beendest du.
- Der RustDesk-Server protokolliert je Verbindung Gerät, Zeitpunkt, Dauer und Anmeldung sowie Dateiübertragungen (Dateiname, Größe, Richtung, keine Inhalte). Das Protokoll wird 12 Monate aufbewahrt. Es ist nicht manipulationssicher, und du hast keine eigene Einsicht darin.
- Eine Videoaufzeichnung der Sitzung gibt es nur bei Bedarf und nur lokal beim Techniker.
- Grundlage ist der AVV von NeckarByte, der Fernwartung und Support abdeckt (Abschnitt 1).

7 Protokollierung

Vier Quellen, jede mit eigenem Zweck und eigener Frist. Keine davon ist ein Mitschnitt von Gesprächen.

QUELLE	INHALT	ZWECK	FRIST	ZUGRIFF
Änderungshistorie	Akteur (Benutzer oder Dienstidentität), Zeitpunkt, Bereich, Aktion (anlegen, ändern, löschen), geändertes Feld mit altem und neuem Wert; Geheimnisse werden maskiert gespeichert	Nachweis, Rollback-Diskussion, Change-Tickets	60 Monate (Standard); der Name der handelnden Person bleibt bis dahin stehen, auch wenn ihr Konto gelöscht ist	Bereichsberechtigung des jeweiligen Bereichs

QUELLE	INHALT	ZWECK	FRIST	ZUGRIFF
Ausführungsverfolgung	je Lauf: Agent, Benutzer, Start/Ende, Erfolg; je Schritt: Tool, Index, Status; je KI-Anfrage: Dienst, Anbieter, Modell, Tokens und deren Quelle, Preis je Richtung, Warte- und Verarbeitungszeit, Drosselung, Zone DSGVO-konform ja/nein. Inhaltsfelder: Fehlertext, Aktenkoffer-Vorschau nur im Debug-Modus des Agenten	Kosten, Kapazität, Fehlersuche, Support-Korrelation	Inhalte 30 Tage, Benutzername 13 Monate, Metadaten dauerhaft (Standard)	Bereich Nutzung / Status
Anwendungslogs	Serverereignisse, Anmeldefehler, abgelehnte API-Schlüssel; Login-Codes, Cookies und Sitzungsschlüssel werden nicht protokolliert	Betrieb, Vorfälle	28 Tage (Standard)	Bereich Status (Live-Log), Dateizugriff auf dem Server
Feedback	Bewertung, Kommentar, gespeicherte Nachricht und Prompt	Qualität	365 Tage (Standard)	Bereich Feedback

Das Protokoll der Fernwartungssitzungen liegt auf dem RustDesk-Server von NeckarByte, nicht in deiner Instanz (Abschnitt 6.3). Für Support-Pakete gilt: Zeitfenster minimal, Geheimnisse und Kundendaten redigieren, Zusammenfassungen und Fehlercodes statt voller Nutzlasten. Logs und Feedback können personenbezogene Daten enthalten; vor einer Weitergabe nach außen gelten deine Datenschutzregeln.

8 Schutz vor Prompt Injection

Texte von außen, also Mails, Anhänge, Webseiten und Dokumente, können Anweisungen an die KI enthalten. MadeForPrivacy prüft sie in jedem KI-Schritt, bevor das Modell sie liest.

- **In jedem KI-Schritt eingebaut.** Bevor ein KI-Tool (Chat, Extraktion, Entscheidung, Klassifikation, Mail, Zusammenfassung) Text an sein Modell schickt, prüft es jedes Eingabe-Item, dessen Text von außen stammen kann: Eingabe und Nachrichten des Benutzers, Mails, Dokumente, Webseiten, Ergebnisse von APIs und Datenbanken, Knowledge-Treffer, Ergebnisse von Subcalls. Geprüft wird genau der Text, den das Modell sieht, auch Werte, die über Platzhalter in einen Prompt eingesetzt werden. Nicht geprüft werden der Systemprompt und die Schrittkonfiguration sowie die Items, die der Server selbst erzeugt (Datum, Benutzer).
- **Prüfmodell je Instanz.** Die Prüfung macht ein KI-Dienst, der auf den KI-Tools als Prüfmodell hinterlegt ist (`guard_ai_service_ids`). Er unterliegt der Datenzone des Schritts wie jeder andere KI-Aufruf: Ein Schritt in Nur lokal kann nie ein Prüfmodell in der Cloud nutzen. Richtet NeckarByte deine Instanz ein, hinterlegt NeckarByte ein zur Zone passendes Prüfmodell. Ohne Prüfmodell prüft der Schritt nichts und schreibt die Warnung `injection_guard_not_configured` ins Log.
- **Markieren statt abbrechen.** Ein Treffer bricht den Lauf nicht ab. Der Text geht als nicht vertrauenswürdige Daten gekennzeichnet in den Prompt, und der Lauf meldet eine Warnung. Kann das Prüfmodell nicht antworten, gilt der Text als „ungeprüft" und wird genauso gekennzeichnet; ungeprüft wird nie zu „sauber".

- **Prüfvermerk ohne Inhalt.** Jedes geprüfte Item trägt einen Vermerk mit Urteil, Prüfsumme des Textes und Version der Prüfung, nie die Begründung des Prüfmodells und nie Inhalt. Ein unveränderter Text wird im nächsten Schritt nicht erneut geprüft. Vermerke, die der Client mitschickt, verwirft der Server.

Flankierend: Das URL-Tool verweigert interne, private und reservierte Adressen (SSRF-Schutz mit Prüfung der tatsächlich verwendeten IP, Ausnahmen nur per Admin-Liste). Aktions-Schaltflächen in Ergebnissen setzt nur die Pipeline aus festen Eigenschaften, nie ein Modell. Der Client öffnet Netzwerkpfade aus Items nur, wenn sie echte UNC-Pfade ohne ausführbare Endungen sind. Kein Prüfmodell erkennt alles, siehe Restrisiken.

9 Betroffenenrechte

Du setzt die Rechte deiner Mitarbeitenden und Kunden um; die Plattform liefert die Hebel.

RECHT	UMSETZUNG IN MADEFORPRIVACY
Auskunft (Art. 15)	Profil und Gruppen des Benutzers (Admin-Bereich Benutzer, Konto-Ansicht im Client), Nutzung je Benutzer, Ausführungsverfolgung nach Benutzername, Gedächtnisse je Benutzer in Knowledge, Handbuch-Historie, Feedback. Konversationen liegen beim Benutzer selbst.
Berichtigung (Art. 16)	Profilfelder kommen aus dem Verzeichnis und werden bei der Anmeldung aktualisiert; manuell gepflegte Felder ändert der Admin. Gedächtniseinträge können gelöscht und neu angelegt werden.
Löschung (Art. 17)	siehe Löschkonzept (5.2): Benutzer löschen, Benutzer aus Nutzungsdaten entfernen, benutzerbezogene Knowledge-Bestände und Dokumente von Hand entfernen, Inhaltsfrist der Verfolgung, Relay-Ablauf, Backup-Retention. Im Änderungsprotokoll bleibt der Name von Admins als Nachweis bis zur Frist (Art. 17 Abs. 3 lit. e DSGVO).
Einschränkung (Art. 18)	Gruppen entziehen, Agenten oder Quellen deaktivieren, Benutzer deaktivieren statt löschen.
Übertragbarkeit (Art. 20)	Manueller Weg, eine Exportfunktion gibt es nicht. Auf Anfrage stellt der Admin die Daten aus den Admin-Ansichten zusammen: Profil, Nutzung je Benutzer, Ausführungsverfolgung, Gedächtnisse in Knowledge. Konversationen, Aufgaben und Entwürfe liegen beim Benutzer; er kann sie im Client als verschlüsselte Sicherung mit eigenem Schlüssel speichern.
Widerspruch (Art. 21)	abhängig von Zweck und Rechtsgrundlage deines Einsatzes; technisch über Einschränkung umsetzbar.
Informationspflichten (Art. 13/14)	Hinweise an Mitarbeitende: welche Agenten laufen, welche Zonen gelten, dass Nutzung je Benutzer ausgewertet wird, dass Porträts aus dem Verzeichnis im Client angezeigt werden. Die Zonenbeschreibungen im Client können wörtlich übernommen werden.

NeckarByte ist an der Umsetzung nicht beteiligt, solange kein Supportvertrag mit Zugriff besteht. Auf Wunsch unterstützen wir bei der Konfiguration der Fristen und bei Löschläufen.

10 Technische und organisatorische Maßnahmen

Nach den Kategorien von Art. 32 DSGVO, nur das, was die Plattform tatsächlich mitbringt. Maßnahmen deiner Infrastruktur (Rechenzentrum, Netz, Endgeräte) kommen hinzu.

KATEGORIE	UMSETZUNG
Zugangskontrolle	Anmeldung über LDAP, Kerberos AD (SSO) oder Entra ID; lokale Benutzer mit bcrypt; Drosselung fehlgeschlagener Anmeldungen; API-Schlüssel mit einmaliger Anzeige und Widerruf; Demo-Anbieter nie produktiv
Zugriffskontrolle	Gruppen aus dem Verzeichnis für Agenten, Knowledge-Quellen, Handbücher, Einstellungsbereiche; serverseitig gesetzte Benutzeridentität im Lauf; persönliche Handbücher und Gedächtnisse je Benutzer
Weitergabekontrolle	Datenzonen je Schritt erzwungen; nur konfigurierte Endpunkte; Webrecherche nur mit geprüften, neutralen Begriffen; SSRF-Schutz; Zugangsdaten nur als Vault-Referenz
Eingabekontrolle	Änderungshistorie je Einstellungsbereich; Ausführungsverfolgung je Lauf, Schritt und KI-Anfrage
Trennungskontrolle	eine Instanz pro Kunde; Gruppen; benutzerbasierte Knowledge-Quellen; Relay-Objekte an erlaubte Benutzer gebunden; Desktop-Vault pro Benutzer
Verschlüsselung	TLS nach außen, mTLS intern (Vault-PKI); AES-256-GCM für das Relay; verschlüsselter Client-Vault (safeStorage/DPAPI); Secrets in Vault; Passwörter als bcrypt
Datenminimierung	Tool-Schritte sehen nur ihre Eingabetypen; Relay-Verweise statt Kopien; Porträts werden auf dem Server nicht gespeichert; keine serverseitigen Konversationen; Fristen für Inhaltsfelder, Benutzernamen, Jobs, Feedback und Änderungshistorie
Integrität	signierter MSI-Installer, Selbst-Update nur bei passender Prüfsumme und Signatur; Relay-IDs als HMAC; Injection-Prüfung in jedem KI-Schritt; Aktions-Schaltflächen nur aus fester Konfiguration
Verfügbarkeit und Belastbarkeit	Ratenlimits je KI-Dienst, Kostenlimits je Gruppe, Parallel-Limit je Benutzer; Job-Recovery nach Neustart; Status- und Health-Ansicht mit Komponentenstatus
Wiederherstellbarkeit	Backup-Skript für Datenbank, Datenordner, Relay, RAGFlow, Vault, Zertifikate mit Prüfsummen und Retention; dokumentierter Restore-Umfang
Überprüfbarkeit	Live-Logs, Änderungshistorie, Nutzungsauswertung je Benutzer und Dienst; Anbieter-Test für Anmeldeanbieter; sicherer Konfigurations-Workflow in der Dokumentation
Auftragskontrolle	du schließt Verträge mit KI-Anbietern selbst; NeckarByte greift nur in einer von dir gestarteten Fernwartungssitzung zu, auf Grundlage des AVV (Muster auf Anfrage), mit Protokoll auf dem RustDesk-Server

11 Restrisiken

Was die Technik nicht wegnimmt und wie du damit umgehst.

RISIKO	WOHER	MINDERUNG
Falsche Zonenzuweisung	Ein Admin weist einem Agenten mit Personendaten die Zone Ungeschützt oder einem externen Dienst die Zone DSGVO-konform ohne AVV zu	Vier-Augen-Prinzip über Bereichsberechtigungen, Änderungshistorie, Zonenprüfung bei Einrichtung und nach Änderungen
KI-Anbieter	Verarbeitung beim Anbieter liegt außerhalb der Plattform	Anbieter mit AVV, EU-Region, Trainingsausschluss; nur die Daten des Schritts
Prompt Injection	Kein Prüfmodell erkennt alle Angriffe; HTML-Mails und Dokumente können versteckten Text tragen. Ohne hinterlegtes Prüfmodell, auch ohne eines in der Zone Nur lokal, prüft ein Schritt nichts	Prüfmodell für jede genutzte Zone hinterlegen und auf die Warnung `injection_guard_not_configured` achten; Treffer gehen gekennzeichnet in den Prompt, keine Aktion ohne Bestätigung, Datenzonen begrenzen den Schaden
Websuche	Neutralisierte Suchbegriffe gehen an externe Suchmaschinen; ein Begriff kann trotz Prüfung Rückschlüsse erlauben. Adressen, die der Benutzer nennt, werden auch in der Zone Nur lokal abgerufen	Websuche nur in Agenten, die sie brauchen; Zone bewusst wählen
Web-Client	Browser-Speicher ohne Vault, keine Trennung in geteilten Profilen	Desktop-Client auf geteilten Rechnern; Browser-Richtlinien
Laufende Sitzung	Entschlüsselte Daten liegen im Arbeitsspeicher, solange jemand angemeldet ist	Sperrbildschirm, Abmelden; Garantie gilt für die Festplatte
Verfolgungs-Vorschauen	Fehlertexte und, im Debug-Modus, Aktenkoffer-Vorschauen können Inhalte tragen	Debug-Modus nur zur Fehlersuche, Frist `retention.debug_content_days` (Standard 30 Tage), Zugriff auf den Bereich Nutzung begrenzen
Logs	können personenbezogene Daten enthalten	28-Tage-Frist, redigierte Support-Pakete
Server-Backups	das Skript `backup-stack.sh` legt DB-Dump und `.env` unverschlüsselt ab; gelöschte Daten leben bis zum Ablauf weiter	verschlüsselter Backup-Speicher, kurze Retention, Zugriff beschränken
Handbuch-Historie	git behält frühere Fassungen; eine Funktion zum Entfernen aus der Historie gibt es nicht	keine personenbezogenen Vorgänge in Handbücher; stehen doch welche darin, legt dein Admin das Handbuch auf Anfrage neu an, damit die Historie verschwindet
Porträts und Profile aus dem Verzeichnis	Übernahme ohne gesonderte Einwilligung (Porträt nur im Client)	Attribut nur mappen, wenn deine Verzeichnisrichtlinie es deckt; Information der Mitarbeitenden

RISIKO	WOHER	MINDERUNG
Benutzerlöschung	Benutzerlöschen entfernt weder die benutzerbezogenen Knowledge-Bestände noch das persönliche Handbuch; der Name bleibt bis zu 13 Monate in den Nutzungsdaten	die beiden manuellen Schritte aus 5.2 in deinen Austrittsprozess aufnehmen; „Benutzer aus Nutzungsdaten entfernen" nutzen
Supportzugriff	Der Techniker sieht in der Sitzung alles, was der angemeldete Admin sieht; das RustDesk-Protokoll ist nicht manipulationssicher und für dich nicht direkt einsehbar	AVV, Sitzung nur nach deiner Freigabe und von dir beendet, kein Konto für NeckarByte, Protokoll 12 Monate

12 Kontakt und Pflege des Dokuments

Dieses Konzept wird mit jedem Release von MadeForPrivacy geprüft und bei Änderungen an Datenflüssen, Speicherorten, Anbietern oder Schutzmaßnahmen aktualisiert. Die jeweils aktuelle Fassung mit Datum steht auf madeforprivacy.de/plattform/datenschutz-mfp/konzept/. Fragen deiner Datenschutzbeauftragten beantworten wir schriftlich, auf Wunsch mit Verweis auf Code und Dokumentation.

NeckarByte UG (haftungsbeschränkt)

Im Roggen 9 · 71636 Ludwigsburg

kontakt@neckarbyte.com · +49 160 98722321 · neckarbyte.com

Ansprechpartner Datenschutz: datenschutz@neckarbyte.com. NeckarByte hat keinen Datenschutzbeauftragten benannt; nach der aktuellen Unternehmensgröße besteht dafür keine Pflicht (§ 38 BDSG).

A Anhang: Einstellungen mit Datenschutzbezug

EINSTELLUNG	STANDARD	WIRKUNG
`retention.relay_hours`	24	Lebensdauer der Relay-Objekte (Nutzlasten, Zustellungen) und der Mailbox-Einträge
`relay.sweep_interval_seconds`	300	Intervall des Bereinigungslaufs (Relay, Mailbox, Logs, Fristen)
`retention.log_days`	28	Löschung der Tages-Logverzeichnisse; 0 = unbegrenzt

EINSTELLUNG	STANDARD	WIRKUNG
`retention.debug_content_days`	30	Entfernt Vorschauen, Fehlertexte und freie Metadaten der Ausführungsverfolgung; Metadaten bleiben; 0 = behalten
`retention.username_months`	13	Entfernt den Benutzernamen aus Läufen, KI-Anfragen und Feedback; Abteilung, Kosten und Tokens bleiben
`retention.metadata_months`	0	Löscht Läufe, Schritte und KI-Anfragen samt Kosten; 0 = behalten
`retention.job_days`	30	Löscht abgeschlossene Jobzeilen; wartende und laufende Jobs nie
`retention.audit_log_months`	60	Löscht Änderungsprotokoll und abgeschlossene Änderungssätze; offene nie
`retention.feedback_days`	365	Löscht Feedback mit gespeicherter Nachricht und Prompt
`retention.client_message_days`	365	Höchstalter von Client-Nachrichten in den Zonen Nur lokal und DSGVO-konform; Zone Ungeschützt ohne zentrale Frist
`app.usage_limits_enabled`, `app.usage_parallel_limit`	aus, 2	Kostenlimits je Gruppe, Parallel-Limit je Benutzer
`app.client_update_enabled`	aus	Selbst-Update des Desktop-Clients über deinen Server (nur signierte Installer)
KI-Dienst: `datazone`	–	Zone des Dienstes; Zugangsdaten als `secret::customer/...`
Agent: `datazone`, `ad_groups`	–	Zone des Agenten, berechtigte Gruppen
KI-Tools: `guard_ai_service_ids`	leer; bei Einrichtung durch NeckarByte belegt	Prüfmodell der Injection-Prüfung; leer = keine Prüfung, Warnung im Log
Mail-Processor: `preserve_html_body`	aus	HTML-Teil der Mail zusätzlich im Item
Knowledge-Quelle: `ad_groups`, `user_based`, `user_deletable`	–	Zugriff, Trennung je Benutzer, Löschung durch Benutzer
`MFP_BACKUP_RETENTION_DAYS`	14	Aufbewahrung der Backups des Skripts

Quellen dieser Fassung: Produktdokumentation (Konzepte Datenzonen, Item-Relay, Lokaler Speicher, Authentifizierung, Knowledge, Mailbox, Job-Scheduler, Handbücher; Admin-Handbuch Logs, Berechtigungen, Backup, Anmeldeanbieter, Nutzung; Einstellungsreferenz), Server-Quellcode (Injection-Prüfung, Porträts, Fristen und Löschläufe, Änderungsprotokoll, Benutzerlöschung, Relay, SSRF-Schutz, Anmeldedrosselung, Webrecherche, Lizenzprüfung), Client-Quellcode (Nachrichtenfrist, Sicherung), Deployment-Vorlage (Dienste, PKI, Backup-Skript), Fernwartung nach der RustDesk-Server-Pro-Dokumentation.