Security-Whitepaper: Benno Cloud Enterprise

Sicherheit, Datenschutz und Compliance bei LWsystems

Stand: 15. Mai 2026

EXECUTIVE SUMMARY: Das Wichtigste auf einen Blick

Dieser Abschnitt fasst die wesentlichen Sicherheits-, Datenschutz- und Compliance-Aspekte von Benno Cloud Enterprise und White Labeled Benno Cloud (WLBC) zusammen. Die vollständigen Details finden sich in den jeweiligen Kapiteln dieses Whitepapers.

Was bietet Benno Cloud Enterprise?

Benno Cloud Enterprise ist der Cloud-Service von LWsystems für revisionssichere E-Mail-Archivierung — betrieben ausschließlich auf Infrastruktur in Deutschland, vollständig unter deutschem Recht.

Kernleistungen:

- Automatische Archivierung aller eingehenden E-Mails nach Maßgabe der jeweiligen Leistungsbeschreibung. Alle E-Mails, die LWsystems über die vereinbarte Schnittstelle erreichen, werden vollautomatisch archiviert. Die Art der Zuführung richtet sich nach der eingesetzten Infrastruktur des Kunden (z.B. Microsoft 365/Exchange Online via Journaling, Self-Hosting-Mailserver, hybride Archivablage, Zimbra SaaS aus der LWsystems Cloud) — Details siehe jeweilige Leistungsbeschreibung: https://www.benno-mailarchiv.de/leistungsbeschreibungen/
- Volltext-Suche und E-Discovery-Funktionen (siehe Kap. 1.4) bei unveränderlicher Archivierung
- Zweifache Verschlüsselung: mandantenspezifisch (AES-256) + Infrastruktur-Ebene (LUKS/AES-256)
- 3-fach redundante Replikation mit 15-Minuten-Intervall und Geo-Redundanz (Nürnberg/Falkenstein)
- Vollständiger Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

White Labeled Benno Cloud (WLBC): Identische technische Infrastruktur, aber unter dem Branding des Reseller-Partners betreibbar. LWsystems agiert dabei als weiterer Auftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO. Details zur Vertragskette und den abweichenden Kommunikationswegen finden sich in Kapitel 6.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

Infrastruktur und Datenschutz

Rechenzentren: Alle Daten werden ausschließlich in Deutschland verarbeitet und gespeichert — in ISO 27001:2022-zertifizierten Rechenzentren der Hetzner Online GmbH (Zertifikatsinhaber: Hetzner Online GmbH) in Nürnberg und Falkenstein. Eine Verarbeitung außerhalb Deutschlands findet nicht statt. (→ Kapitel 2)

Redundanz: Drei physisch separate Server-Nodes in verschiedenen Rechenzentrumsabschnitten bilden eine Active-Active-Active-Architektur. Eingehende E-Mails werden auf dem primären Node gespeichert und automatisch im 15-Minuten-Intervall auf alle drei Nodes repliziert. Bei Ausfall eines Nodes arbeiten die verbleibenden Nodes weiter. Es werden keine klassischen Backups erstellt — die 3-fach redundante Replikation ersetzt dieses Konzept. (→ Kapitel 2.2)

Verschlüsselung: Zwei unabhängige Verschlüsselungsebenen nach dem Defense-in-Depth-Prinzip:

1. *Ebene 1:* Jeder Mandant verfügt über sein eigenes kryptographisches Schlüsselpaar (RSA) für seine archivierten E-Mails. Die archivierten E-Mails werden AES-256-verschlüsselt. Bei Vertragsende wird dieser Schlüssel vernichtet — die Daten werden damit sofort und unwiederbringlich unlesbar (Crypto Erase).
2. *Ebene 2:* Alle Dateisysteme sind vollständig per LUKS mit AES-256 im XTS-Modus verschlüsselt. Selbst bei physischem Zugriff auf die Hardware bleiben Daten geschützt.

Die Übertragung erfolgt über TLS in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2) mit Forward Secrecy für alle Verbindungen. TLS 1.0 und 1.1 sind deaktiviert. (→ Kapitel 3)

Compliance-Anforderungen

DSGVO: LWsystems schließt mit jedem Direktkunden einen vollständigen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO ab. Die technischen und organisatorischen Maßnahmen (TOMs) sind auf die Anforderungen von Art. 32 DSGVO ausgerichtet und werden regelmäßig überprüft. Datenpannen werden LWsystems unverzüglich von Hetzner gemeldet und von LWsystems unverzüglich an den Kunden weitergeleitet. (→ Kapitel 5.1, 7)

GoBD: Benno Cloud Enterprise stellt die technische Grundlage für GoBD-konforme Archivierung bereit: Unveränderbarkeit archivierter E-Mails, Vollständigkeit, Nachvollziehbarkeit, maschinelle Auswertbarkeit (Volltext-Suche) und Revisionssicherheit. LWsystems stellt den Systemteil der Verfahrensdokumentation zur Verfügung.

Wichtiger Hinweis: Die steuerrechtliche Verantwortung für die Ordnungsmäßigkeit der Archivierung verbleibt gemäß GoBD Rz. 21 immer beim Steuerpflichtigen — auch bei vollständiger technischer Auslagerung. LWsystems übernimmt den weitaus größten Teil der Umsetzungsleistungen; die formale Verantwortung und einige organisatorische Maßnahmen (z.B. Unterzeichnung der Verfahrensdokumentation, interne Zugriffsregelungen) verbleiben beim Kunden. (→ Kapitel 5.4)

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

§ 203 StGB (Berufsgeheimnisträger): Alle Mitarbeiter von LWsystems mit potenziellem Datenzugriff sind auf die strafrechtliche Schweigepflicht nach § 203 Abs. 1 i.V.m. Abs. 3 Satz 2 StGB verpflichtet; schriftliche Verpflichtungserklärungen und Schulungsnachweise liegen vor. Benno Cloud Enterprise ist in der Standardkonfiguration nicht für Mandanten ausgelegt, die eine Verarbeitung von Daten nach § 203 StGB erfordern — die vertraglichen Rahmenbedingungen mit unserem Infrastrukturpartner Hetzner lassen dies in der aktuellen Betriebsform nicht zu. Anfragen von Berufsgeheimnisträgern klären wir individuell. (→ Kapitel 5.3, 10.3)

Sicherheitsmaßnahmen im Überblick

Zugriffskontrolle: Maximal 3–5 namentlich bekannte Administratoren mit SSH-Key-Authentifizierung. Alle privilegierten Zugriffe (sudo/root, SSH-Logins) werden protokolliert. Zugriff auf Kundendaten erfolgt ausschließlich für Systemadministration oder auf ausdrückliche Anfrage des Kunden — nicht zur inhaltlichen Einsichtnahme. Technisch ist ein vollständiger Ausschluss administrativer Zugriffe nicht möglich; dieser Umstand wird transparent kommuniziert und durch mehrere Schutzschichten (technisch, organisatorisch, rechtlich) abgesichert. (→ Kapitel 4)

Netzwerksicherheit: Jeder Server nutzt einen host-basierten Paketfilter (iptables/nftables) nach dem Prinzip „Default Deny" — nur explizit benötigte Ports sind geöffnet. Hetzner bietet zusätzlich einen automatisierten DDoS-Schutz auf Netzwerkebene (Hetzner setzt auf netzwerkseitige DDoS-Erkennung und -Mitigation durch dedizierte Hardware-Lösungen. Details zu den eingesetzten Systemen sind in Hetzners Sicherheitsdokumentation beschrieben, siehe https://www.hetzner.com/de/unternehmen/ddos-schutz/). Eine zentrale Netzwerk-Firewall ist nicht vorhanden; der kombinierte Schutz aus Host-Firewalls und DDoS-Mitigation bietet ein hohes Sicherheitsniveau ohne Single Point of Failure. (→ Kapitel 2.4, 9)

Incident Management: Bei Sicherheitsvorfällen besteht eine dokumentierte Meldekette: Hetzner meldet unverzüglich an LWsystems, LWsystems meldet unverzüglich an den Kunden (bzw. bei WLBC: an den Reseller).

Mitarbeiterverpflichtungen: Alle Mitarbeiter werden vor Tätigkeitsbeginn auf das Datengeheimnis nach DSGVO verpflichtet. Alle Mitarbeiter mit potenziellem Datenzugriff werden regelmäßig — mindestens jährlich — zu § 203 StGB geschult. Neue Mitarbeiter werden vor Tätigkeitsbeginn geschult. (→ Kapitel 10)

Vertragsende und Datenlöschung

Mit Vertragsende werden alle mandantenspezifischen Daten (E-Mails, Metadaten, Konfigurationen, Suchindizes) vollständig gelöscht. Die kryptographische Löschung erfolgt durch Vernichtung des mandantenspezifischen Verschlüsselungsschlüssels — die Daten werden damit sofort unlesbar, ohne dass eine physische Überschreibung aller Speicherblöcke erforderlich ist.

System-Logs mit Einträgen mehrerer Mandanten werden zeitbasiert rotiert (90–180 Tage bzw. 12 Monate für Archivierungsprotokolle) — eine selektive Löschung mandantenspezifischer Einträge aus gemischten Logs ist technisch nicht praktikabel.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

Auf Anfrage stellen wir die archivierten E-Mails in portablen, entschlüsselten Formaten (.eml) zur Verfügung. Die konkreten Abläufe (Fristen, Formate, Übergabe) werden im Einzelfall mit dem Kunden vereinbart. (→ Kapitel 8)

Wo finde ich Details?

Thema	Kapitel
Infrastruktur, Rechenzentren, Redundanz	Kapitel 2
Verschlüsselung und Schlüsselverwaltung	Kapitel 3
Zugriffskontrolle und Administratorzugriffe	Kapitel 4
DSGVO, GoBD, § 203 StGB	Kapitel 5
Auftragsverarbeitung, Subunternehmer, WLBC-Vertragsketten	Kapitel 6
Incident Management und Meldepflichten	Kapitel 7
Datenlöschung und Datenportabilität	Kapitel 8
Netzwerksicherheit und Firewall	Kapitel 9
Mitarbeiterverpflichtungen und Schulungen	Kapitel 10
Audits, Zertifizierungen, Kontrollrechte	Kapitel 11
FAQ (häufige Fragen)	Kapitel 12
Kontakt und Ansprechpartner	Kapitel 13

Zu GoBD-Kundenpflichten, Aufbewahrungsfristen und steuerrechtlichen Anforderungen empfehlen wir ergänzend das Whitepaper „Rechtliche Aspekte zur E-Mail-Archivierung": www.benno-mailarchiv.de/rechtliche-aspekte.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

RECHTLICHE HINWEISE UND HAFTUNGSAUSSCHLUSS

Zweck dieses Dokuments

Dieses Whitepaper dient ausschließlich der allgemeinen Information über die Sicherheitsarchitektur von Benno Cloud Enterprise und White Labeled Benno Cloud. Es stellt weder ein rechtsverbindliches Angebot noch einen Vertragsbestandteil dar.

Keine Rechtsberatung

Die in diesem Dokument enthaltenen Informationen ersetzen nicht die individuelle rechtliche, technische oder datenschutzrechtliche Beratung durch qualifizierte Fachexperten.

Vertragliche Verbindlichkeit

Maßgeblich sind ausschließlich:

- Der individuell geschlossene Service-Vertrag
- Die Auftragsverarbeitungsvereinbarung (AVV)
- Unsere Allgemeinen Geschäftsbedingungen (AGB)
- Service Level Agreement (SLA)

Aktualität

Rechtsstand: Rechtslage zum 18. Februar 2026 (veröffentlicht 2026). Wesentliche berücksichtigte Rechtsänderungen: BEG IV (ab 1.1.2025), Data Act (Verordnung (EU) 2023/2854), GoBD in der Fassung vom 14.7.2025.

Letzte Aktualisierung: 06. März 2026

Zwischen Aktualisierungen kann es zu Abweichungen zwischen diesem Whitepaper und der tatsächlichen Infrastruktur kommen. Im Zweifelsfall erfragen Sie den aktuellen Stand bei: datenschutz@lw-systems.de

Urheberrecht

© 2026 LWsystems GmbH & Co. KG. Alle Rechte vorbehalten.

Die Vervielfältigung, Bearbeitung oder kommerzielle Nutzung ohne vorherige schriftliche Zustimmung ist nicht gestattet.

Vertraulichkeit

Dieses Dokument ist öffentlich verfügbar und unterliegt keinen Vertraulichkeitsbeschränkungen.

Erlaubte Nutzung:

- Einsicht für Evaluierungszwecke

- Weitergabe an Dritte für Audits/RFPs (mit Quellenangabe)
- Interne Verwendung bei Bestandskunden

Nicht gestattet ist:

- Die Bearbeitung oder Veränderung des Dokuments ohne Kennzeichnung
- Die kommerzielle Verwertung ohne Zustimmung von LWsystems
- Die Verwendung als eigenes Sicherheitskonzept ohne entsprechende Anpassung (gilt insbesondere für Reseller)

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

1. Einleitung

1.1 Begriffsbestimmungen

In diesem Whitepaper werden die Begriffe ‚weiterer Auftragsverarbeiter' (DSGVO-Terminologie) und ‚Unterauftragnehmer' (üblicher Sprachgebrauch) synonym verwendet. Rechtsverbindlich ist Art. 28 Abs. 4 DSGVO.

1.2 Über dieses Dokument

Dieses Whitepaper dokumentiert die Sicherheitsarchitektur, Datenschutzmaßnahmen und Compliance-Anforderungen für **Benno Cloud Enterprise** und **White Labeled Benno Cloud (WLBC)**, unseren Cloud-Service, der die technische Grundlage für GoBD-konforme E-Mail-Archivierung bereitstellt.

Zielgruppe

Benno Cloud Enterprise:

- Direktkunden von LWsystems GmbH & Co. KG
- IT-Verantwortliche und Datenschutzbeauftragte
- Compliance-Officer und Revisoren
- Entscheidungsträger bei der Auswahl von Cloud-Diensten und/oder E-Mail-Archivierungslösungen

White Labeled Benno Cloud (WLBC):

- Reseller-Partner, die den Service unter eigenem Branding anbieten
- IT-Dienstleister und Managed Service Provider (MSP)
- Cloud-Service-Provider mit Portfolio-Erweiterung

Hinweis für Reseller-Partner

Dieses Dokument beschreibt die technische Infrastruktur, Sicherheitsmaßnahmen und Compliance-Anforderungen, die LWsystems als weiterer Auftragsverarbeiter (Unterauftragnehmer) gemäß Art. 28 Abs. 4 DSGVO für die White Label-Lösung bereitstellt.

Reseller-Partner können dieses Whitepaper:

- Als Grundlage für eigene Sicherheitsdokumente nutzen
- In Audits und RFPs (Request for Proposal) referenzieren
- Auf Anfrage an Endkunden weitergeben
- Für interne Compliance-Nachweise verwenden

Wichtig: Die beschriebene Infrastruktur und Sicherheitsarchitektur gilt unverändert für alle WLBC-Instanzen. Vertragliche Beziehungen und Support-Kontakte bestehen zwischen dem Reseller und seinen Endkunden – LWsystems agiert als weiterer Auftragsverarbeiter des Kun-

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

den im Sinne von Art. 28 Abs. 4 DSGVO.

Geltungsbereich

Dieses Dokument gilt für alle Benno Cloud Enterprise und White Labeled Benno Cloud Instanzen, die auf der Infrastruktur von LWsystems betrieben werden. Die technischen Details, Verschlüsselungsmethoden, Sicherheitsmaßnahmen und Compliance-Anforderungen sind für beide Varianten identisch.

Struktur des Dokuments

1. **Einleitung:** Über LWsystems, Benno Cloud Enterprise und dieses Dokument
2. **Infrastruktur und Hosting:** Rechenzentren, Redundanz, physische Sicherheit
3. **Verschlüsselung und Schlüsselverwaltung:** Mehrschichtige Verschlüsselung, kryptographische Verfahren
4. **Zugriffskontrolle und Berechtigungen:** Technische und organisatorische Maßnahmen
5. **Datenschutz und Compliance:** DSGVO, GoBD, branchenspezifische Anforderungen
6. **Auftragsverarbeitung und Subunternehmer:** Vertragsketten, weiterer Auftragsverarbeiter (Unterauftragnehmer)
7. **Incident Management: Meldeprozesse, Response-Verfahren**
8. **Datenlöschung und Vertragsende:** Löschprozesse, kryptographische Löschung
9. **Netzwerksicherheit:** Firewall, DDoS-Schutz, Transportverschlüsselung
10. **Mitarbeiterverpflichtungen:** Schulungen, Schweigepflicht
11. **Audits und Zertifizierungen:** Kontrollrechte, Nachweise
12. **FAQ:** Häufig gestellte Fragen
13. **Kontakt:** Ansprechpartner für Direktkunden und Reseller

Aktualität

Dieses Dokument wird regelmäßig aktualisiert, um Änderungen in der Infrastruktur, rechtlichen Anforderungen oder Sicherheitsstandards zu berücksichtigen. Die jeweils aktuelle Version ist auf unserer Website verfügbar: www.benno-mailarchiv.de

1.3 Über LWsystems

LWsystems GmbH & Co. KG ist ein deutsches IT-Dienstleistungsunternehmen mit Sitz in Bad Iburg, spezialisiert auf Open Source IT-Lösungen und digitale Souveränität. Wir bieten Alternativen zu Microsoft, Google und anderen Tech-Konzernen und setzen dabei auf:

- **Datenschutz by Design:** Lösungen aus Deutschland — entwickelt nach den Grundsätzen von Privacy by Design und Privacy by Default (Art. 25 DSGVO)
- **Open Source**: Transparenz, Kontrolle, keine Vendor-Lock-ins

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

- **Digitale Souveränität**: Unabhängigkeit von US-Cloud-Anbietern

1.4 Benno Cloud Enterprise

Benno Cloud Enterprise ist unser Cloud-Service für revisionssichere E-Mail-Archivierung — als technische Grundlage für die GoBD-konforme Nutzung durch den Kunden (insbes. für Microsoft 365/Exchange Online).

Der Service bietet:

- Automatische Archivierung aller E-Mails
- Volltext-Suche und E-Discovery-Funktionen (siehe unten)
- Technische Grundlage für GoBD-, DSGVO- und branchenspezifisch-konforme Nutzung
- 3-fach redundante Speicherung mit Geo-Redundanz in Deutschland
- **Zweifache Verschlüsselung:** Mandantenspezifische Verschlüsselung + Infrastruktur-Verschlüsselung (siehe Kapitel 3 unten)

E-Discovery-Funktionen

Benno Cloud Enterprise bietet praxisorientierte E-Discovery-Funktionen für den täglichen Einsatz durch alle Mitarbeiter — keine spezialisierte Legal-Software, sondern produktive Suchwerkzeuge direkt im Browser:

Mandantenweite Volltext-Suche: Suche über alle archivierten E-Mails inkl. Anhänge in ca. 1.300 unterstützten Dateiformaten, typischerweise in 1–2 Sekunden auch bei Millionen archivierter E-Mails

Permalink: Jede angezeigte E-Mail erhält einen eindeutigen, dauerhaften Link zur direkten Referenzierung — z.B. im Betriebsprüfungsfall oder bei internen Compliance-Prüfungen. Standardmäßig ist der Zugriff auf eingeloggte Benno-Nutzer mit entsprechenden Rechten beschränkt; systemweit kann alternativ ein öffentlicher Zugriff ohne Login aktiviert werden (für jeden erreichbar, der den Benno-Server auf Port 443 erreicht)

Weiterleitung: Eine angezeigte E-Mail kann direkt aus dem Archiv an eine beliebige E-Mail-Adresse weitergeleitet werden — mit originalem Absender, Empfänger und Zeitstempel. Hinweis: Die Mail wird mit dem originalen Absendezeitpunkt zugestellt und erscheint beim Empfänger chronologisch eingeordnet, nicht als neue Mail

EML-Export: Jede angezeigte E-Mail kann als EML-Datei heruntergeladen oder direkt im lokalen Mail-Client geöffnet werden (z.B. zur Beantwortung oder Weiterleitung aus dem originalen Kontext heraus)

Abgrenzung: Benno-E-Discovery ist kein Legal-Hold-System, kein Custodian-Management und kein Litigation-Support-Tool im Sinne von US-amerikanischen E-Discovery-Plattformen (z.B. Relativity, Nuix). Der Funktionsumfang ist auf den deutschen Unternehmensalltag ausgerichtet: GoBD-Betriebsprüfung, DSGVO-Auskunftspflichten und interne Compliance-Anforderungen.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

1.5 White Labeled Benno Cloud (WLBC)

White Labeled Benno Cloud ist die Reseller-Variante von Benno Cloud Enterprise. Sie ermöglicht es IT-Dienstleistern, Managed Service Providern und Cloud-Anbietern, eine vollständig unter eigenem Branding betriebene E-Mail-Archivierungslösung anzubieten.

Technische Basis

WLBC nutzt die **identische technische Infrastruktur** wie Benno Cloud Enterprise:

- Automatische E-Mail-Archivierung mit Unterstützung gängiger Schnittstellen (Journaling, REST-API, u.a.)
- Volltext-Suche und E-Discovery-Funktionen (siehe Kapitlel 1.4)
- Technische Grundlage für GoBD-, DSGVO- und branchenspezifisch-konforme Nutzung
- 3-fach redundante Speicherung mit Geo-Redundanz in Deutschland
- **Zweifache Verschlüsselung:** Mandantenspezifische Verschlüsselung + Infrastruktur-Verschlüsselung (siehe Kapitel 3)

White Label Funktionen

Zusätzlich bietet WLBC:

- **Vollständiges Rebranding:** Web-Interface, E-Mails und Benachrichtigungen im Corporate Design des Resellers
- **Eigene Domains:** Zugriff über eine eigene Domain (z.B. archiv.reseller-name.de)
- **Mandantenfähigkeit:** Verwaltung mehrerer Endkunden über eine zentrale Oberfläche
- **Reseller-Portal:** Zentrale Administration und Verwaltung aller Kunden-Instanzen

Vertragsmodell

Rolle von LWsystems:

LWsystems agiert als **weiterer Auftragsverarbeiter** (Unterauftragnehmer) gemäß Art. 28 Abs. 4 DSGVO des Resellers und stellt die technische Infrastruktur bereit.

Vertragskette:

Endkunde (Verantwortlicher) → Reseller (Auftragsverarbeiter) → LWsystems (weiterer Auftragsverarbeiter)

Für Endkunden:

Aus Sicht der Endkunden ist der Service eine Lösung des Resellers. LWsystems bleibt im Hintergrund und wird (je nach Vereinbarung mit dem Reseller) in der Liste weiterer Auftragsverarbeiter (Unterauftragnehmer-Liste) der AVV genannt.

Vorteile für Reseller

- **Schneller Markteintritt:** Keine eigene Infrastruktur-Entwicklung erforderlich
- **Skalierbarkeit:** Von einzelnen Mandanten bis zu hunderten Kunden

- **Sicherheit und Compliance:** Reseller profitieren von der durch uns genutzten Infrastruktur der Hetzner Online GmbH (ISO 27001:2022-zertifiziert)
- **Support-Modell:** Reseller übernehmen den First-Level-Support

Geltungsbereich dieses Whitepapers

Dieses Sicherheits-Whitepaper gilt **unverändert** für White Labeled Benno Cloud (WLBC). Die beschriebenen technischen Maßnahmen, Verschlüsselungsverfahren, Sicherheitskonzepte und Compliance-Anforderungen sind identisch mit Benno Cloud Enterprise.

Unterschiede bestehen lediglich in:

- Vertraglichen Beziehungen (siehe Kapitel 6)
- Kontrollrechten (siehe Kapitel 11)
- Kommunikationswegen (siehe Kapitel 13)

2. Infrastruktur und Hosting

2.1 Rechenzentrumsstandort

Alle Daten befinden sich ausschließlich in Deutschland.

- **Standorte**: Hetzner Online GmbH, Rechenzentren in Nürnberg und Falkenstein
- **Keine Datenverarbeitung außerhalb Deutschlands**: Alle Verarbeitungs- und Speichervorgänge finden ausschließlich in deutscher Infrastruktur statt
- **Rechtssicherheit**: Anwendbares Recht ist deutsches und europäisches Datenschutzrecht. Da ausschließlich deutsche Unternehmen als Anbieter und Unterauftragnehmer eingesetzt werden (LWsystems GmbH & Co. KG, Hetzner Online GmbH), bestehen keine vertraglichen Beziehungen zu US-amerikanischen Unternehmen, auf die der US CLOUD Act Anwendung finden könnte.

2.2 Redundanz und Hochverfügbarkeit

3-fach redundante Infrastruktur

Benno Cloud Enterprise wird auf einer hochverfügbaren Cluster-Architektur betrieben:

- **3 physisch separate Server-Nodes** in verschiedenen Rechenzentrumsabschnitten
- **Datenreplikation**: Alle Daten werden automatisch im 15-Minuten-Intervall auf alle drei Nodes repliziert
- **Active-Active-Active:** Alle Nodes sind jederzeit aktiv und verarbeiten Anfragen
- **Load Balancing**: Verteilung der Last für optimale Performance
- **Verfügbarkeit**: 99,3% während der vereinbarten Verfügbarkeitszeit gemäß SLA (Annex A unserer AGB). Rechtsverbindlich sind ausschließlich die im SLA definierten Parameter.

Automatische Hochverfügbarkeit:

Bei Ausfall eines Nodes arbeiten die beiden verbleibenden Nodes normal weiter. Neue Daten werden temporär 2-fach (statt 3-fach) redundant gespeichert. Nach Wiederherstellung des ausgefallenen Nodes erfolgt automatisch eine Re-Synchronisation der zwischenzeitlich hinzugekommenen Daten.

Vorteil gegenüber klassischen Backups:

Aspekt	Klassisches Backup	Unsere 3-fach Redundanz
Datenverlust-Risiko	Bis zu 24 h (je nach Backup-Frequenz)	Maximal 15 Minuten (Replikationsintervall)
Recovery Time	Stunden bis Tage	Keine - läuft kontinuierlich weiter
Aktualität	Veraltet (letzter Backup-Stand)	Immer aktuell
Service-Ausfall	Ja (während Restore)	Nein (transparent)

Für E-Mail-Archivierung ist dieses Replikationsintervall ohne praktische Relevanz: Ein Datenverlust könnte allenfalls E-Mails der letzten 15 Minuten vor einem simultanen Ausfall aller drei Nodes betreffen — ein konstruktiv nahezu ausgeschlossenes Szenario. Gegenüber klassischen Backups mit bis zu 24 Stunden Datenverlust-Risiko bedeutet dies eine Verbesserung um den Faktor 96.

2.3 Physische Sicherheit (Hetzner-Rechenzentren)

Hetzner Online GmbH betreibt ISO 27001:2022-zertifizierte Rechenzentren (Zertifikatsinhaber: Hetzner Online GmbH), u.a. mit:

- **Zutrittskontrolle**: Elektronisches Zutrittskontrollsystem mit Protokollierung
- **Videoüberwachung**: Flächendeckende Überwachung aller sicherheitsrelevanten Bereiche
- **Perimetersicherheit**: Hochsicherheitszaun mit Übersteig- und Untergrabenschutz
- **Brandschutz**: Früherkennungssysteme, automatische Alarmierung, dynamisches Brandschutzkonzept
- **Stromversorgung**: Redundante USVs und Notstromaggregate (NEA)
- **Kühlung**: Redundante Kühlsysteme mit kontinuierlicher Temperaturüberwachung
- **24/7-Überwachung**: Ständig besetztes Sicherheitspersonal

Die vollständige Liste der Sicherheitsmaßnahmen ist in **Kapitel 6 (Abschnitt „Sicherheitsmaßnahmen bei Hetzner")** aufgeführt.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

2.4 Netzwerksicherheit

DDoS-Schutz

Hetzner bietet kostenlosen, automatisierten DDoS-Schutz (basierend auf dedizierten Hardware-Lösungen. Details siehe Hetzners Sicherheitsdokumentation: https://www.hetzner.com/de/unternehmen/ddos-schutz/), der Angriffe wie DNS-Reflection, SYN Floods und UDP Floods erkennt und innerhalb weniger Sekunden filtert.

Firewall

Jeder Server nutzt einen konfigurierten Paketfilter (iptables/nftables) nach dem Prinzip "Default Deny" – nur explizit benötigte Ports (SMTP, HTTPS, SSH) sind geöffnet. Diese host-basierten Paketfilter sind das primäre Sicherheitsinstrument auf Netzwerkebene. Eine zentrale Netzwerk-Firewall ist nicht implementiert.

3. Verschlüsselung und Schlüsselverwaltung

3.1 Mehrschichtige Verschlüsselung bei der Ablage (Data at Rest)

Benno Cloud Enterprise setzt auf ein **zweistufiges Verschlüsselungskonzept** nach dem Stand der Technik **(Defense in Depth)**:

Ebene 1: Mandantenspezifische Verschlüsselung

- Für jeden Mandanten wird ein eigenes kryptographisches RSA-Schlüsselpaar erzeugt. Die archivierten E-Mails werden AES-256-verschlüsselt, wobei der symmetrische AES-Schlüssel mandantenspezifisch durch das RSA-Verfahren geschützt wird.
- Jede archivierte E-Mail wird damit mandantenspezifisch verschlüsselt
- Bei Vertragsende: Kryptographische Löschung durch Vernichtung des Mandantenschlüsselpaares

Ebene 2: Infrastruktur-Verschlüsselung (LUKS) (Linux Unified Key Setup)

- Vollverschlüsselung aller Dateisysteme mit AES-256 in XTS-Modus
  (Umfang: Alle Anwendungsdaten, archivierte E-Mails, Suchindex, Verschlüsselungsschlüssel)
- Schutz vor physischem Zugriff auf Hardware
- Manuelle Entsperrung nach Systemneustart erforderlich

Vorteil der doppelten Verschlüsselung:

- Selbst bei Kompromittierung einer Verschlüsselungsebene bleiben die Daten geschützt
- Mandantentrennung auch auf kryptographischer Ebene
- Compliance mit höchsten Sicherheitsanforderungen (z.B. Gesundheitswesen, Behörden)

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

3.2 Verschlüsselungsschlüssel-Verwaltung

Wo befinden sich die Verschlüsselungsschlüssel?

Die Verschlüsselungsschlüssel für die E-Mail-Archive befinden sich standardmäßig in unserer Infrastruktur, da wir diese für den Betrieb des Cloud-Service benötigen:

- **Speicherort**: Auf jedem der drei Server-Nodes im verschlüsselten LUKS-Dateisystem
- **Zugriff**: Nur nach manueller Entsperrung durch autorisierte Administratoren
- **Verwendung**: Für Archivierung, Indizierung, Suchfunktionen und Anzeige der E-Mails

Verfügbare Optionen:

- **Standardbetrieb**: Die Schlüssel verbleiben in unserer verschlüsselten Infrastruktur. Wir können den Service vollumfänglich betreiben.
- **Schlüssel-Hinterlegung**: Auf individuelle Anfrage kann eine Schlüsselkopie zur sicheren Aufbewahrung durch den Kunden vereinbart werden. Die konkreten Bedingungen, Verfahren und Verantwortlichkeiten werden im Einzelfall vertraglich geregelt.

3.3 Hardware-Sicherheitsmodule (HSM)

Frage: Werden die Schlüssel in HSM verwaltet?

Antwort: Nein. Für E-Mail-Archivierung ist der Einsatz von Hardware-Sicherheitsmodulen nicht erforderlich und würde keinen nennenswerten Sicherheitsgewinn bei erheblichen Mehrkosten bieten.

Vergleich:

Aspekt	LUKS-Verschlüsselung	HSM
Verschlüsselungsstärke	AES-256	AES-256
Schutz vor physischem Zugriff	Ja	Ja
Manipulationsschutz	Ja (verschlüsselte Filesystems)	Ja (tamper-proof Hardware)
Kosten	Standard	Sehr hoch (Hardware + Wartung)
Compliance	DSGVO, BSI, GoBD	DSGVO, BSI, GoBD
Typischer Einsatz	Cloud-Services, Storage	Payment-Systeme, PKI, Behörden

Wann ist HSM sinnvoll?

- Payment-Verarbeitung (PCI DSS Level 1)
- Zertifizierungsstellen (Root CAs)
- Behörden mit VS-NfD-Daten oder höher
- Finanztransaktionen mit sehr hohen Volumen

Unser Ansatz bietet ein **angemessenes und bewährtes** Sicherheitsniveau für E-Mail-Archi-

vierung, das den Anforderungen der DSGVO, des BSI und gängiger Compliance-Standards entspricht.

3.4 Verschlüsselung bei der Übertragung (Data in Transit)

TLS-Verschlüsselung für alle Verbindungen

TLS wird in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2) verwendet. TLS 1.0 und 1.1 sind deaktiviert.

- **Web-Interface**: HTTPS/TLS
- **E-Mail-Empfang**: SMTP mit STARTTLS
- **API-Zugriffe**

Details zur SMTP-Transportverschlüsselung:

Wenn (bspw.) Microsoft 365/Exchange Online Journal-Mails zu uns sendet bzw. E-Mails per SMTP zugeleitet werden:

- **Protokoll**: SMTP über TLS (STARTTLS)
- **TLS-Version**: TLS wird in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2) verwendet. TLS 1.0 und 1.1 sind deaktiviert.
- **Cipher Suites**: Es werden ausschließlich Cipher Suites eingesetzt, die den aktuellen BSI-Empfehlungen (TR-02102-2) entsprechen und Perfect Forward Secrecy (PFS) unterstützen.
- **Forward Secrecy**: Ja (PFS aktiviert)

Warum TLS 1.2 als Minimum?

- Ältere TLS-Versionen haben bekannte Sicherheitslücken
- Microsoft 365 hat TLS 1.0/1.1 seit Oktober 2020 deaktiviert
- BSI-Empfehlung: Mindestens TLS 1.2
- DSGVO-Konformität: “Stand der Technik” erfordert TLS 1.2+

Wie wird die TLS-Version ausgehandelt?

1. Sender schickt “ClientHello” mit unterstützten Versionen
2. Unser Server wählt die höchste gemeinsam unterstützte Version

4. Zugriffskontrolle und Berechtigungen

4.1 Administrative Zugriffe

Wer hat Zugriff auf die Systeme?

- **Anzahl**: Maximal 3-5 namentlich bekannte Administratoren
- **Authentifizierung**: SSH-Key-basiert

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

- **Protokollierung**: Alle privilegierten Zugriffe (sudo/root) werden protokolliert
- **Zugriffsberechtigungen:**
  - Root-Zugriff nur für Systemadministration
  - Anwendungs-Ebene: Separate Accounts mit eingeschränkten Rechten

4.2 Schutz vor unbefugtem Zugriff durch LWsystems

Transparenz ist uns wichtig:

Wie bei jedem professionellen Hosting- oder Cloud-Service haben autorisierte Administratoren technisch die Möglichkeit zum Systemzugriff – dies ist für Betrieb, Wartung und Support unverzichtbar. **Ein vollständiger technischer Ausschluss ist nicht möglich**, da wir sonst den Service nicht betreiben könnten.

Unser mehrschichtiger Schutzansatz:

1. Technische Maßnahmen:

- Vollverschlüsselte Systeme (LUKS)
- Manuelle Entsperrung nach jedem Neustart erforderlich
- Strenge Zugriffsbeschränkungen (nur wenige autorisierte Personen)
- Protokollierung aller Systemzugriffe

2. Organisatorische Maßnahmen:

- Verpflichtung aller Mitarbeiter auf das Datengeheimnis (DSGVO)
- Verpflichtung aller Mitarbeiter mit potenziellem Datenzugriff auf die strafrechtliche Schweigepflicht nach § 203 StGB (→ Kapitel 5.3)
- Need-to-know-Prinzip: Zugriff nur soweit erforderlich
- Regelmäßige Datenschutzschulungen

3. Rechtliche Absicherung:

- Auftragsverarbeitungsvertrag mit klaren Pflichten
- Strafrechtliche Konsequenzen bei Missbrauch (§ 202a StGB, § 42 BDSG)
- Für Healthcare-Projekte: Strafrechtliche Schweigepflicht nach § 203 Abs. 1 i.V.m. Abs. 3 Satz 2 StGB; zivilrechtliche Haftung für Vertragsverletzungen nach §§ 280 ff. BGB

4. Praktische Umsetzung:

- Administratoren greifen ausschließlich für Systemadministration oder auf ausdrückliche Anfrage des Kunden zu — nicht zur inhaltlichen Einsichtnahme in E-Mails

5. Zugriffsprotokollierung:

- Alle privilegierten Systemzugriffe (root/sudo, SSH-Logins) werden automatisch protokolliert.

- LUKS-Entsperrungen nach System-Reboots (implizite Protokollierung: Ohne LUKS-Entsperrung können keine Services gestartet werden. Laufende Services bedeuten erfolgreiche LUKS-Entsperrung)
- Direkter Archivzugriff auf Mandantendaten auf Anwendungsebene erfolgt ausschließlich auf dokumentierte Kundenanfrage und wird protokolliert. Zur Protokollierbarkeit der LUKS-Systemebene und deren technischen Grenzen siehe den nachfolgenden Hinweis. Einzelheiten zur Protokollierung, Integritätssicherung und Aufbewahrung sind in den internen Prozessdokumenten geregelt.

Hinweis zur LUKS-Entsperrung:

Eine direkte Protokollierung der LUKS-Entsperrung ist technisch nicht möglich, da das verschlüsselte Dateisystem vor der Entsperrung nicht beschreibbar ist. Die erfolgreiche Entsperrung lässt sich jedoch durch Systemboot-Logs und den erfolgreichen Start der Systemdienste (z.B. Benno MailArchiv) nachweisen, da diese nur bei verfügbarem (und entschlüsseltem) Dateisystem starten können. Diese indirekte Nachweisbarkeit ist technisch bedingt und wird im Rahmen der Gesamtschutzarchitektur (verschlüsselte Systeme, Zugriffsprotokollierung auf Anwendungsebene, dokumentierte Betriebsprozesse) als ausreichend eingestuft.

4.3 Kundenspezifische Zugriffe

Zugriff auf Ihre Archive:

- **Web-Interface**: Über HTTPS mit Benutzername/Passwort + optional 2FA
- **Berechtigungskonzept**: Rollenbasierte Zugriffssteuerung (RBAC)
- **Single Sign-On**: Optionale Integration mit Identity Provider des Kunden (OAuth 2.0)
- **API-Zugang**: Für Self-Hosting-Installationen verfügbar; für Benno Cloud Enterprise in Vorbereitung (geplante Erweiterung — kein vertraglicher Anspruch).

Rollen im Endkunden-Archiv

Jeder Mandant verwaltet seine Archiv-Nutzer über drei vordefinierte Rollen:

Rolle	Berechtigung
USER	Zugriff ausschließlich auf E-Mails der dem Nutzer zugeordneten Mailadressen und Wildcard-Aliase
REVISOR	Vollzugriff auf das gesamte Archiv des Mandanten (Vollzugriff für Revisionszwecke — z.B. Betriebsprüfung durch Finanzamt oder Steuerberater bzw. Wirtschaftsprüfer)
ADMIN	Benutzerverwaltung: Anlegen, Bearbeiten und Löschen von Nutzern sowie Zuweisung von Berechtigungen

Neu angelegte Benutzer erhalten standardmäßig die Rolle USER (Privacy by Default). Erweiterte Rollen (REVISOR, ADMIN) werden ausschließlich durch einen bestehenden ADMIN des Mandanten vergeben. LWsystems hat keinen Zugriff auf die mandantenspezifische Benutzerverwaltung.

5. Datenschutz und Compliance

5.1 DSGVO — Auftragsverarbeitung und Datenschutzmaßnahmen

LWsystems erbringt seine Leistungen als Auftragsverarbeiter auf Basis eines vollständigen Auftragsverarbeitungsvertrags nach Art. 28 DSGVO und stellt die vertraglichen und technischen Grundlagen für den DSGVO-konformen Einsatz durch den Kunden bereit:

- **Art. 28 DSGVO – Auftragsverarbeitung:**
  - Dokumentierter Auftragsverarbeitungsvertrag (AVV)
  - Technische und organisatorische Maßnahmen (TOMs) implementiert
  - Unterstützung bei Betroffenenrechten (inkl. Löschung einzelner E-Mails nach Art. 17 DSGVO auf schriftliche Weisung des Kunden; Self-Service-Funktion in der Anwendung ist geplant)
  - Meldepflichten bei Datenpannen
  - Kontrollrechte des Auftraggebers
- **Art. 32 DSGVO - Sicherheit der Verarbeitung:**
  - Verschlüsselung (Data at Rest (mit Defense in Depth) + Data in Transit)
  - Pseudonymisierung der Infrastruktur-Metadaten (wo technisch anwendbar; für archivierte E-Mail-Inhalte nicht möglich, da Volltext-Suche und GoBD-konforme Lesbarkeit Klartext erfordern)
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
  - Regelmäßige Überprüfung und Bewertung
- **Art. 33 DSGVO - Meldepflicht bei Datenpannen:**
  - Incident-Response-Prozess etabliert
  - Unverzügliche Meldung an Auftraggeber
  - Dokumentation aller Sicherheitsvorfälle

5.2 Verarbeitungsverzeichnis

Wir führen ein vollständiges Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO:

- **Zweck der Verarbeitung:** E-Mail-Archivierung
- **Kategorien betroffener Personen:** Mitarbeiter, Kunden, Partner des Auftraggebers
- **Kategorien personenbezogener Daten:** E-Mail-Inhalte, Metadaten, Kommunikationsdaten
- **Kategorien von Empfängern:** Keine (außer auf Weisung)
- **Drittlandübermittlungen:** Keine
- **Fristen für Löschung:** Bei Vertragsende vollständige Löschung gemäß § 9 AVV. Ge-

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

setzliche Aufbewahrungsfristen können einer sofortigen Löschung entgegenstehen und liegen in der Verantwortung des Kunden als Verantwortlichem (§ 147 AO, § 257 HGB; Details in Kapitel 5.4).

5.3 Berufsgeheimnisträger (§ 203 StGB)

Benno Cloud Enterprise ist in der Standardkonfiguration nicht für Mandanten ausgelegt, die eine Verarbeitung von Daten nach § 203 StGB erfordern — die vertraglichen Rahmenbedingungen mit unserem Infrastrukturpartner Hetzner lassen dies in der aktuellen Betriebsform nicht zu. Anfragen von Berufsgeheimnisträgern klären wir individuell.

Besondere Anforderungen im Gesundheitswesen, bei Anwälten, Steuerberatern:

Für Projekte mit Berufsgeheimnisträgern gelten erhöhte Anforderungen:

- **§ 203 StGB:** Alle Mitarbeiter mit potenziellem Datenzugriff sind explizit auf die strafrechtliche Schweigepflicht nach § 203 Abs. 1 i.V.m. Abs. 3 Satz 2 StGB verpflichtet
- **Strafbarkeit**: Bei unbefugter Offenbarung droht Freiheitsstrafe bis zu einem Jahr oder Geldstrafe
- **Schulung**: RegelmäßigeSchulung aller Mitarbeiter zu § 203 StGB und DSGVO
- **Dokumentation**: Schriftliche Verpflichtungserklärungen liegen für alle relevanten Mitarbeiter vor
- **Status als "mitwirkende Personen":** Unsere Mitarbeiter gelten kraft Gesetzes als mitwirkende Personen im Sinne von **§ 203 Abs. 3 Satz 2 StGB** und unterliegen damit unmittelbar der strafrechtlichen Schweigepflicht nach **§ 203 Abs. 1 StGB**.

5.4 GoBD — Leistungsumfang und Kundenpflichten

Benno Cloud Enterprise unterstützt Kunden bei der Erfüllung der Anforderungen der GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form, BMF-Schreiben in der Fassung vom 14. Juli 2025)

Verantwortlichkeit

Die steuerrechtliche Verantwortung für die Ordnungsmäßigkeit der elektronischen Buchführung und Archivierung verbleibt gemäß GoBD Rz. 21 beim Steuerpflichtigen — auch bei vollständiger technischer Auslagerung an LWsystems. LWsystems kann diese Verantwortung weder übernehmen noch dem Kunden abnehmen.

Leistungsumfang von LWsystems

Als technischer Betreiber übernimmt LWsystems den weitaus größten Teil der GoBD-Umsetzungsleistungen:

- Unveränderbarkeit im Sinne der GoBD (Rz. 64 ff.): Archivierte E-Mails werden durch SHA-256-Prüfsummen gegen unerkannte Veränderungen gesichert — Änderungen wären erkennbar und nachvollziehbar.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

- Vollständigkeit und Nachvollziehbarkeit der Archivierung
- Revisionssichere Protokollierung
- Maschinelle Auswertbarkeit (Volltext-Suche)
- Infrastruktur für die Einhaltung der gesetzlichen Aufbewahrungsfristen
- Bereitstellung des Systemteils der Verfahrensdokumentation (GoBD Rz. 151–155)

Kundenpflichten

Kundenseitig verbleiben folgende organisatorische Pflichten:

- Einrichtung der E-Mail-Zuführung (z.B. Journal-Mailbox in Microsoft 365, DNS-/MX-Konfiguration)
- Formale Unterzeichnung und Verantwortungsübernahme der Verfahrensdokumentation
- Interne organisatorische Regelungen (z.B. Umgang mit privater E-Mail-Nutzung)
- Verwaltung der eigenen Zugriffsrechte im System

LWsystems berät und unterstützt Kunden bei allen organisatorischen Schritten.

Verfahrensdokumentation (GoBD Rz. 151–155)

Die GoBD verpflichten jeden Steuerpflichtigen zur Erstellung und Pflege einer Verfahrensdokumentation. LWsystems stellt den Systemteil der Verfahrensdokumentation für Benno Cloud Enterprise bereit, der die technischen Aspekte des Archivsystems vollständig beschreibt. Der Kunde unterzeichnet die Verfahrensdokumentation formal und ist für die Ergänzung der organisatorischen Teile sowie der kundenseitigen technischen Konfiguration (z.B. E-Mail-Zuführung, Journal-Mailbox, DNS-/MX-Einrichtung) verantwortlich.

Betriebsprüfung (§ 147 Abs. 6 AO)

Bei einer steuerlichen Betriebsprüfung muss der Kunde dem Finanzamt Zugang zu den archivierten Daten ermöglichen. Der Kunde kann dem Finanzamt oder dem Steuerberater über die Benno Cloud WebApp jederzeit selbst Zugang einrichten (Revisor-Rolle). LWsystems unterstützt auf Wunsch des Kunden bei der Archivsuche in Abstimmung mit dem Prüfer; der Aufwand wird nach tatsächlichem Zeitaufwand berechnet, sofern nicht im Einzelfall eine abweichende Vereinbarung getroffen wird. LWsystems stellt die systemseitige Betreiber-Verfahrensdokumentation dem Finanzamt auf Anforderung zur Verfügung. Der Kunde sollte LWsystems frühzeitig über eine laufende Betriebsprüfung informieren. Die Einzelheiten werden im Vertrag und in der Verfahrensdokumentation geregelt.

5.5 Branchenspezifische Compliance

Je nach Branche unterstützen wir Kunden bei der Erfüllung weiterer branchenspezifischer Anforderungen:

Gesundheitswesen: Für Projekte im Gesundheitswesen gelten die erhöhten Anforderungen nach § 203 StGB (siehe Kapitel 5.3). Darüber hinaus stellt die mandantenspezifische Verschlüsselung sicher, dass Patientendaten technisch isoliert und vor unbefugtem Zugriff ge-

schützt sind. Für Compliance-Nachweise steht das optionale Audit-Log zur Verfügung (→ Kapitel 5.6).

Finanzsektor: Die technische Infrastruktur von Benno Cloud Enterprise unterstützt die Anforderungen regulierter Umgebungen: revisionssichere Archivierung, Unveränderbarkeit, Volltext-Suche und Nachvollziehbarkeit. Ob und inwieweit die spezifischen MaRisk-Anforderungen des Kunden erfüllt werden, ist durch den Kunden gemeinsam mit seiner Compliance-Funktion zu prüfen — LWsystems stellt hierfür die erforderliche technische Dokumentation bereit. Für Finanzunternehmen, die unter DORA (Verordnung (EU) 2022/2554, anwendbar seit 17.01.2025) fallen, sind ergänzende vertragliche Vereinbarungen nach Art. 30 DORA auf Anfrage möglich. Die DORA-Compliance-Verantwortung verbleibt beim Finanzunternehmen als reguliertem Institut.

Öffentliche Verwaltung: Benno Cloud Enterprise erfüllt die datenschutzrechtlichen Anforderungen nach DSGVO und BDSG. Die ausschließliche Datenhaltung in Deutschland (Hetzner-Rechenzentren) entspricht den Anforderungen vieler öffentlicher Auftraggeber an digitale Souveränität und Datensicherheit.

5.6 Audit-Log für Archivzugriffe

Benno Cloud Enterprise bietet optional ein Audit-Log für Suchabfragen im Archiv, das für alle Kunden in hochregulierten Bereichen aktivierbar ist (z.B. Gesundheitswesen, Finanzsektor, öffentliche Verwaltung). Eine Erweiterung des Funktionsumfangs ist geplant.

Hinweis zum Audit-Trail:

Benno Cloud Enterprise bietet optional ein Audit-Log für Suchabfragen im Archiv. Dieses Feature ist standardmäßig deaktiviert (Privacy by Default). Bei Aktivierung protokolliert das System pro Benutzer:

- Zeitpunkt der Suchabfrage
- Verwendete Suchbegriffe und gesetzte Filter
- Abgefragter Container (Archiv-Segment, sofern genutzt)

Nicht protokolliert werden gegenwärtig, welche E-Mails aus der Trefferliste geöffnet oder heruntergeladen wurden. Eine Erweiterung des Audit-Logs um diese Aktionen ist geplant.

Datenschutzrechtliche Hinweise:

Die Aktivierung des Audit-Logs erfordert beim Kunden:

- Rechtsgrundlage (z.B. berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO)
- Information der betroffenen Mitarbeiter (Transparenzpflicht)
- Ggf. Betriebsvereinbarung (§ 87 Abs. 1 Nr. 6 BetrVG)
- Zweckbindung und Aufbewahrungsfristen

Die datenschutzrechtliche Verantwortung für die Protokollierung liegt beim Kunden als Verantwortlichem (Art. 4 Nr. 7 i.V.m. Art. 24 DSGVO).

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

Beispiele für typische Anwendungsfälle:

- IT-Sicherheit: Erkennung unbefugter Zugriffe
- § 203 StGB-Compliance: Nachvollziehbarkeit von Suchabfragen im Archiv
- GoBD-Compliance: Protokollierung von Suchabfragen als ergänzender Nachweis im Prüfungsfall
- Forensik: Aufklärung bei Verdacht auf Datenmissbrauch

Empfohlene Maßnahmen:

- Betriebsvereinbarung abschließen (wenn Betriebsrat vorhanden)
- Mitarbeiter schriftlich informieren (Transparenzgebot)
- Zugriff auf Audit-Log beschränken (IT-Sicherheit, Datenschutzbeauftragter)
- Aufbewahrungsfrist begrenzen (z.B. 90 Tage)
- Zweckbindung dokumentieren

LWsystems berät auf Wunsch bei der technischen Implementierung des Audit-Logs.

6. Auftragsverarbeitung und Subunternehmer

6.1 Rechtsgrundlage und Vertragsketten

Benno Cloud Enterprise (Direktvertrieb)

Bei Benno Cloud Enterprise besteht eine direkte vertragliche Beziehung zwischen dem Kunden und LWsystems als Auftragsverarbeiter gemäß Art. 28 DSGVO.

Vertragskette:

Endkunde (Verantwortlicher) → LWsystems (Auftragsverarbeiter) → Unterauftragnehmer (z.B. Hetzner)

White Labeled Benno Cloud (Reseller-Modell)

Bei White Labeled Benno Cloud agiert LWsystems als weiterer Auftragsverarbeiter (Unterauftragnehmer) des Reseller-Partners gemäß Art. 28 Abs. 4 DSGVO.

Vertragskette:

Endkunde (Verantwortlicher) → Reseller (Auftragsverarbeiter) → LWsystems (weiterer Auftragsverarbeiter) → Unterauftragnehmer (z.B. Hetzner)

Wichtig: Der Reseller ist gemäß § 6 lit. b unserer AVV (gegenüber LWsystems) sowie gemäß Art. 28 Abs. 4 DSGVO und seinem eigenen AVV mit dem Endkunden verpflichtet, seine Endkunden über LWsystems als weiteren Auftragsverarbeiter zu informieren und diesen ein Widerspruchsrecht einzuräumen.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

6.2 Eingesetzte weitere Auftragsverarbeiter (Unterauftragnehmer)

LWsystems setzt für den Betrieb von Benno Cloud Enterprise und White Labeled Benno Cloud folgende Unterauftragnehmer ein:

Name	Anschrift	Leistung	Standort	Zertifizierung
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen	Anmietung dedizierter Server (Root-Server)	Nürnberg / Falkenstein	ISO 27001:2022

Leistungsumfang:
Hetzner stellt die physische Hardware (Dedicated Server) sowie die Rechenzentrumsinfrastruktur bereit. Die Konfiguration, Administration, Verschlüsselung und alle darauf laufenden Anwendungen (Benno MailArchiv) werden vollständig durch LWsystems betrieben.

Auftragsverarbeitungsvertrag:
Mit Hetzner besteht ein dokumentierter Auftragsverarbeitungsvertrag, der die Anforderungen von Art. 28 DSGVO erfüllt.

Hetzner AVV verfügbar unter:
https://www.hetzner.com/de/rechtliches/avv

Technische und organisatorische Maßnahmen (TOMs):
https://www.hetzner.com/de/rechtliches/tom

6.3 Keine weiteren Subunternehmer bei Benno Cloud Enterprise

Hinweis zur Unterauftragnehmer-Situation:

Für Verträge ab Frühjahr 2025 wird ausschließlich Hetzner Online GmbH als Unterauftragnehmer eingesetzt. Der Auftragsverarbeitungsvertrag von LWsystems (Stand 30.01.2024) enthält in Anlage 3 noch einen Eintrag für die gridscale GmbH (S3-Objektspeicher), der ausschließlich Bestandsverträge aus der Zeit vor Frühjahr 2025 betrifft. Für alle ab Frühjahr 2025 geschlossenen Verträge liegt die vollständige Datenhaltung bei Hetzner; gridscale wird für diese Verträge nicht eingesetzt.

Abgrenzung zu anderen LWsystems-Produkten:

Bei anderen Produkten von LWsystems können zusätzliche Auftragsverarbeiter (Unterauftragnehmer) eingesetzt werden. Diese sind **nicht Bestandteil** von Benno Cloud Enterprise oder White Labeled Benno Cloud.

Für die in diesem Whitepaper beschriebenen Services gilt:

- Hetzner Online GmbH (Dedicated Server, Rechenzentrum)
- Kein Cloud-Objektspeicher-Dienst
- Keine weiteren Hosting-Provider
- Keine sonstigen Dienstleister

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

6.4 Informationspflichten bei Änderungen

Benno Cloud Enterprise

Gemäß § 6 lit. b unserer AVV informieren wir Kunden über beabsichtigte Änderungen in Bezug auf weitere Auftragsverarbeiter (Unterauftragnehmer):

LWsystems informiert Kunden über beabsichtigte Änderungen bei Unterauftragnehmern gemäß § 6 AVV rechtzeitig vor deren Einsatz. Kunden haben ein Widerspruchsrecht innerhalb von zwei Wochen nach Information. Ohne Widerspruch innerhalb dieser Frist gelten die Änderungen als genehmigt. Wird kein Einvernehmen erzielt, gelten die Regelungen des § 6 lit. c AVV. Die konkreten Kommunikationswege und Prozessschritte sind in den internen Prozessdokumenten geregelt.

White Labeled Benno Cloud

Für White Labeled Benno Cloud gilt die gleiche Regelung: LWsystems informiert Reseller-Partner mit denselben Fristen und Widerspruchsrechten. Der Reseller ist verpflichtet, seine Endkunden gemäß seiner eigenen AVV weiterzuinformieren.

6.5 Prüfung und Auswahl von weiteren Auftragsverarbeitern

LWsystems wählt Unterauftragnehmer sorgfältig aus und prüft:

Technische Kriterien

- ISO 27001:2022 Zertifizierung (oder gleichwertig)
- Physische Sicherheit der Rechenzentren
- Redundanz der Infrastruktur
- Verfügbarkeitszusagen (SLA)
- Netzwerksicherheit (DDoS-Schutz, Firewall)

Datenschutzrechtliche Kriterien

- Standort in Deutschland/EU/EWR
- Dokumentierter Auftragsverarbeitungsvertrag (AVV)
- Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO
- Nachweis über Datenschutz-Management
- Incident-Response-Prozesse

Vertragliche Absicherung

- AVV mit gleichwertigen Datenschutzverpflichtungen
- Kontrollrechte (Audits, Zertifikate)
- Haftungsregelungen
- Regelungen zur Datenlöschung bei Vertragsende

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

- Informationspflichten bei Sicherheitsvorfällen

6.6 Haftung

Benno Cloud Enterprise

LWsystems haftet Kunden gegenüber für die Einhaltung der Datenschutzpflichten durch Unterauftragnehmer nach Maßgabe der Haftungsregelungen des Hauptvertrags (§ 10 lit. a AVV i.V.m. § 11 AGB Cloud Services) sowie im Außenverhältnis nach Art. 82 DSGVO.

White Labeled Benno Cloud

Haftungskette:

Der Reseller-Partner haftet Endkunden gegenüber für die Einhaltung der Datenschutzpflichten nach Maßgabe seines eigenen Vertrags mit dem Endkunden sowie gemäß Art. 82 DSGVO.

LWsystems haftet dem Reseller gegenüber für die Einhaltung der Datenschutzpflichten durch Unterauftragnehmer nach Maßgabe der Haftungsregelungen des Hauptvertrags (§ 10 lit. a AVV i.V.m. § 11 AGB Cloud Services) sowie Art. 82 DSGVO (z.B. Hetzner).

6.7 Standorte der Datenverarbeitung

Alle Datenverarbeitung erfolgt ausschließlich in Deutschland:

- **Primärer Standort:** Hetzner Rechenzentrum Nürnberg
- **Sekundärer Standort:** Hetzner Rechenzentrum Falkenstein
- **Geo-Redundanz:** Zwischen den Standorten

Keine Datenverarbeitung in Drittstaaten:

- Keine Server außerhalb der EU/EWR
- Kein administrativer Zugriff aus Drittstaaten
- Keine Datenübertragung außerhalb Deutschlands

Gemäß § 2 unserer AVV ist die Verarbeitung personenbezogener Daten auf Deutschland beschränkt. Eine Verarbeitung in Ländern außerhalb der EU oder des EWR findet nicht statt.

6.8 Kontrolle der weiteren Auftragsverarbeiter (Unterauftragnehmer)

LWsystems übt regelmäßige Kontrolle über die eingesetzten Unterauftragnehmer aus:

Regelmäßige Überprüfung

LWsystems überprüft eingesetzte Unterauftragnehmer regelmäßig auf Einhaltung der vereinbarten Datenschutzpflichten (Art. 28 Abs. 3 lit. h DSGVO), insbesondere hinsichtlich der Aktualität von Zertifizierungen und TOMs. Frequenz und Umfang der Überprüfung sind in den internen Prozessdokumenten geregelt.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

Kontinuierliches Monitoring

- Verfügbarkeitsüberwachung (24/7)
- Performance-Monitoring
- Sicherheitsupdates und Patch-Management
- Incident-Tracking

Dokumentation

- Alle Prüfergebnisse werden dokumentiert
- Zertifikate und Testate werden archiviert
- Bei Audits auf Anfrage verfügbar

6.9 Zusammenfassung

Aspekt	Benno Cloud Enterprise	White Labeled Benno Cloud
Vertragspartner	Direktvertrag mit LWsystems	Vertrag mit Reseller
Rolle von LWsystems	Auftragsverarbeiter (Art. 28 DSGVO)	Weiterer Auftragsverarbeiter (Art. 28 Abs. 4 DSGVO)
Unterauftragnehmer	Hetzner Online GmbH	Hetzner Online GmbH (identisch)
Informationspflicht	Direkt an Endkunden	An Reseller → Reseller an Endkunden
Widerspruchsrecht	Direkt gegenüber LWsystems	Gegenüber Reseller → Reseller gegenüber LWsystems
Haftung	LWsystems gegenüber Endkunden	Reseller gegenüber Endkunden, LWsystems gegenüber Reseller
Technische Infrastruktur	Gleiche Infrastruktur, gleiche Verschlüsselung und gleiche Sicherheitsmaßnahmen für alle Mandanten	Gleiche Infrastruktur, gleiche Verschlüsselung und gleiche Sicherheitsmaßnahmen für alle Mandanten
Standort	Deutschland (Nürnberg/Falkenstein)	Deutschland (Nürnberg/Falkenstein)

6.10 Meldeprozess bei Sicherheitsvorfällen

Der vollständige Incident-Response-Prozess und die Meldepflichten sind in Kapitel 7 geregelt.

Umfang der Meldung durch Hetzner (gemäß § 9 Abs. 1 lit. b AVV mit Hetzner): Hetzner ist vertraglich verpflichtet, LWsystems unverzüglich zu informieren. Die Meldung umfasst mindestens: Art der Verletzung, Kategorien und ungefähre Anzahl betroffener Personen und Datensätze, Name und Kontaktdaten des Datenschutzverantwortlichen bei Hetzner, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

LWsystems leitet diese Information unverzüglich an den Kunden weiter — bei WLBC an den Reseller, der sie unverzüglich an den Endkunden weitergibt. Details zur Meldekette und zu den Reaktionsfristen → Kapitel 7.

6.11 Sicherheitsmaßnahmen bei Hetzner

Hetzner Online GmbH betreibt ISO 27001:2022-zertifizierte Rechenzentren mit umfassenden Sicherheitsmaßnahmen:

Physische Sicherheit

- **ISO 27001:2022-Zertifizierung** der Rechenzentren Nürnberg und Falkenstein
- **24/7 technischer Support vor Ort** durch qualifiziertes Personal
- **Elektronische Zutrittskontrolle** mit Videoüberwachung und Protokollierung aller Zutrittsversuche
- **Hochsicherheitszäune** und perimetrische Absicherung des Rechenzentrumsgeländes
- **Brandschutzsysteme** (automatische Löschanlagen, Rauchmelder, Brandmeldeanlage)
- **Klimatisierung und Überwachung** der Umgebungsbedingungen (Temperatur, Luftfeuchtigkeit)

Netzwerksicherheit

- **Dauerhaft aktive DDoS-Erkennung** (Hetzner setzt auf dedizierte Hardware-Lösungen. Details zu den eingesetzten Systemen sind in Hetzners Sicherheitsdokumentation beschrieben, siehe https://www.hetzner.com/de/unternehmen/ddos-schutz/).
- **Redundante Netzwerkinfrastruktur** mit mehreren Upstream-Providern
- **Möglichkeit zur individuellen Firewall-Konfiguration** am Switch-Port (über Hetzner Robot)
- **Traffic-Monitoring** und Anomalie-Erkennung
- **Automatische Mitigation** bei erkannten DDoS-Angriffen

Verfügbarkeit und Redundanz

- **Redundante USVs** (Unterbrechungsfreie Stromversorgung)
- **Notstromaggregate** mit automatischer Umschaltung bei Stromausfall
- **Redundante Kühlsysteme** zur Vermeidung von Überhitzung
- **Umfassendes Brandschutzkonzept** mit automatischen Löschsystemen
- **Redundante Netzwerkanbindung** an verschiedene Provider

Hardware-Entsorgung

Gemäß Hetzner AVV, Anlage 2 (Technische und organisatorische Maßnahmen):

- Definiertes Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung
- Rückstandsfreies Löschen durch hardwaregestützte Löschmethode
- Physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung
- Vernichtung erfolgt im Rechenzentrum Falkenstein nach ISO/IEC 21964
- Sichere Transportbehälter bei Datenträger-Transport zwischen Standorten

Zusätzliche Maßnahmen durch LWsystems

Auf Serverebene implementieren wir als LWsystems zusätzliche Sicherheitsmaßnahmen, die über die Hetzner-Infrastruktur hinausgehen:

Zugriffsschutz:

- Restriktive Firewall-Konfiguration (Host-basierter Paketfilter, Default Deny)
- SSH-Zugriff nur mit Schlüsselpaaren (keine Passwort-Authentifizierung)
- Beschränkung auf autorisierte IP-Adressen

Verschlüsselung:

- LUKS-Verschlüsselung aller Dateisysteme (AES-256)
- Mandantenspezifische Verschlüsselung der archivierten E-Mails
- TLS für alle Netzwerkverbindungen (TLS wird grundsätzlich in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2) verwendet. TLS 1.0 und 1.1 sind deaktiviert)

Betrieb und Wartung:

- Regelmäßige Sicherheitsupdates für Betriebssystem und Anwendungen
- Monitoring und Alerting
- Backup-Strategie (nur Server-Konfiguration)
- 3-fach redundante Datenspeicherung (statt klassischer Backups)
- Anwendungssicherheit (Härtung, regelmäßige Sicherheitsüberprüfungen)
- Protokollierung aller administrativen Zugriffe

Nachweise

Für Audits und Compliance-Nachweise stehen folgende Dokumente zur Verfügung:

- **ISO 27001:2022-Zertifikat (Hetzner):** Auf Anfrage über Hetzner verfügbar
- **TOMs (Technische und organisatorische Maßnahmen):** Dokumentiert im Hetzner AVV, Anlage 2
- **Hetzner AVV:** https://www.hetzner.com/de/rechtliches/avv
- **Hetzner TOMs:** https://www.hetzner.com/de/rechtliches/tom

- **LWsystems Verfahrensdokumentation:** Auf Anfrage verfügbar (beschreibt zusätzliche Sicherheitsmaßnahmen auf Serverebene)

Anforderung von Dokumenten:

Benno Cloud Enterprise: datenschutz@lw-systems.de

White Labeled Benno Cloud (Reseller): datenschutz@lw-systems.de

White Labeled Benno Cloud (Endkunden): Kontakt über den Reseller-Partner

7. Incident Management und Meldeprozesse

7.1 Meldepflicht bei Datenschutzverletzungen

Rechtsgrundlage: § 8 unserer AVV + Art. 33 DSGVO

Meldepflicht:

Wir sind verpflichtet, Kunden **unverzüglich** zu benachrichtigen, wenn wir Kenntnis erlangen von:

- Zufälliger oder unbefugter Zerstörung personenbezogener Daten
- Verlust von Daten
- Unbefugter Änderung von Daten
- Unbefugter Offenlegung von Daten
- Unbefugtem Zugriff auf personenbezogene Daten

"**Unverzüglich**" **bedeutet:** Ohne schuldhaftes Zögern nach Kenntniserlangung, entsprechend § 8 unserer AVV.

7.2 Umfang der Meldung

Unsere Meldung umfasst mindestens:

1. Beschreibung der Verletzung:
   - Art der Verletzung (unbefugter Zugriff, Datenverlust, etc.)
   - Kategorien der betroffenen Personen (soweit bekannt)
   - Ungefähre Zahl der betroffenen Personen (soweit bekannt)
   - Betroffene Kategorien personenbezogener Daten
   - Ungefähre Zahl der betroffenen Datensätze
2. Kontaktdaten des Ansprechpartners für Datenschutzfragen
   - Anlaufstelle für weitere Informationen
3. Folgenabschätzung:
   - Beschreibung der wahrscheinlichen Folgen

4. Gegenmaßnahmen:
    - Ergriffene Maßnahmen zur Behebung
    - Vorgeschlagene Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen

7.3 Incident-Response-Prozess

Bei Verdacht auf einen Sicherheitsvorfall durchläuft LWsystems einen dokumentierten Incident-Response-Prozess: Erkennung und Erstbewertung des Vorfalls, Eindämmungsmaßnahmen zur Schadensbegrenzung, unverzügliche Meldung an betroffene Kunden, Ursachenanalyse und Beseitigung sowie Nachbereitung zur Prozessverbesserung. Die genauen Verantwortlichkeiten, Eskalationsstufen und Dokumentationspflichten sind in den internen Prozessdokumenten geregelt.

7.4 Unterstützung bei Meldepflichten

Gemäß § 4 lit. d unserer AVV unterstützen wir Kunden in angemessenem Umfang bei:

- Benachrichtigung der Aufsichtsbehörden (Art. 33 DSGVO)
- Benachrichtigung betroffener Personen (Art. 34 DSGVO)
- Bereitstellung aller relevanten Informationen
- Dokumentation für Nachweispflichten

8. Datenlöschung und Vertragsende

8.1 Löschung nach Vertragsende

Rechtsgrundlage: § 9 unserer AVV

Mit Beendigung des Vertrages erlischt die Rechtsgrundlage für die Datenverarbeitung. Wir sind verpflichtet, sämtliche im Auftrag verarbeiteten personenbezogenen Daten unverzüglich zu löschen.

Unterschiedliche Szenarien:

Benno Cloud Enterprise:

- Der Kunde meldet das Vertragsende direkt an LWsystems (Kündigung).

White Labeled Benno Cloud:

- **Vertragsende Reseller ↔ LWsystems:**
  Alle Daten des Resellers (inkl. aller Endkunden) werden gelöscht.
- **Vertragsende Endkunde ↔ Reseller:**
  Der Reseller meldet LWsystems das Vertragsende über das WLBC Reseller-Portal.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

Datenvorhaltung vor Löschung:

Nach Bestätigung durch LWsystems werden die Daten für einen angemessenen Übergangszeitraum vorgehalten, um eine Datenübergabe gemäß Data Act (Verordnung (EU) 2023/2854) zu ermöglichen.

Die konkreten Fristen werden im Einzelfall zwischen Reseller und LWsystems vereinbart. Die endgültige Löschung erfolgt nach Ablauf des vereinbarten Zeitraums.

Datenübergabe vor Löschung:

Auf Anfrage stellen wir die archivierten E-Mails als Download-Paket zur Verfügung (siehe Kapitel 8.4 für Details zur Datenportabilität). LWsystems weist Kunden und Reseller im Zuge der Vertragsbeendigung auf die Möglichkeit der Datenübergabe hin.

Umfang der Löschung:

Die folgenden Daten werden nach Vertragsende gelöscht:

- **Alle archivierten E-Mails und Anhänge**
- **Sämtliche Konfigurationen und Metadaten** (Benutzerkonten, Einstellungen, Verwaltungszugriffe)
- **Sämtliche temporären Verarbeitungsdaten**
- **Datenbank-Einträge** (alle mandantenspezifischen Einträge und Verknüpfungen)
- **Volltext-Suchindizes** und Ordnerstrukturen

System-Logs und Protokolldateien:

System-Logs (z.B. SMTP-Empfangslogs, Zugriffsprotokolle) enthalten technische Metadaten wie E-Mail-Adressen von Absendern und Empfängern, Zeitstempel und Verbindungsinformationen, jedoch **keine E-Mail-Inhalte**.

Da diese Logs für den Betrieb einer sicheren und stabilen IT-Infrastruktur unerlässlich sind und technisch bedingt Einträge mehrerer Mandanten enthalten, erfolgt deren Löschung **zeitbasiert** nach folgenden Aufbewahrungsfristen:

Log-Typ	Aufbewahrungsfrist	Zweck
SMTP-Empfangslogs	90 Tage	Debugging, Fehleranalyse, Compliance-Nachweis
System-Zugriffslogs	90 Tage	IT-Sicherheit, Audit-Trail
Sicherheitslogs	180 Tage	Angriffserkennung, forensische Analyse
Archivierungsprotokolle	12 Monate	GoBD-Nachweis, rechtliche Absicherung — Einzelheiten sind in den internen Prozessdokumenten von LWsystems geregelt

Die Logs werden durch automatische Log-Rotation nach Ablauf dieser Fristen unwiederbringlich gelöscht.

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

Vorteile der zeitlich begrenzten Aufbewahrung von System-Logs:

Die zeitlich begrenzte Aufbewahrung von System-Logs ist erforderlich für:

1. **IT-Sicherheit:** Erkennung von Angriffen, Anomalien und Missbrauchsversuchen über mehrere Mandanten hinweg
2. **Systemstabilität:** Debugging, Performance-Analyse und Fehlerdiagnose
3. **Compliance-Nachweis:** Nachweis der ordnungsgemäßen technischen Verarbeitung und Zustellung; soweit SMTP-Logs als Nachweisgrundlage für Archivierungsprotokolle nach GoBD Rz. 119 ff. dienen, kann ergänzend Art. 6 Abs. 1 lit. c DSGVO i.V.m. § 147 AO als Rechtsgrundlage herangezogen werden
4. **Rechtliche Absicherung:** Dokumentation bei Streitigkeiten über Empfang oder Verarbeitung von E-Mails

Die Aufbewahrung von System-Logs erfolgt nach dem Prinzip der Datensparsamkeit, da:

- Logs ausschließlich technische Metadaten enthalten, keine E-Mail-Inhalte
- Der Zugriff streng auf autorisierte Administratoren beschränkt ist
- Die Aufbewahrungsfristen auf das technisch und rechtlich erforderliche Minimum begrenzt sind
- Eine sofortige selektive Löschung mandantenspezifischer Einträge aus gemischten Logfiles technisch nicht praktikabel ist und die Integrität der Logs sowie die IT-Sicherheit aller Mandanten gefährden würde
- Keine anderweitige Nutzung oder Auswertung der Log-Daten erfolgt

Ausnahme:

Eine Löschung unterbleibt, soweit wir aufgrund gesetzlicher Vorgaben oder behördlicher Anordnung zur Aufbewahrung verpflichtet sind (z.B. steuerrechtliche Aufbewahrungsfristen für Rechnungen, anhängige rechtliche Auseinandersetzungen). In diesen Fällen werden die betroffenen Daten gesperrt und nur noch für den spezifischen Zweck verarbeitet.

8.2 Technische Durchführung der Löschung

Mehrstufiger Löschprozess:

1. Logische Löschung auf Mandantenebene

- Entfernung aller Daten des betreffenden Mandanten aus dem aktiven Archiv
- Löschung des gesamten Mandanten-Ordnerbaums
- Löschung aller zugehörigen Metadaten und Konfigurationen
- Deaktivierung aller Zugänge

2. Kryptographische Löschung (Crypto Erase)

Mandantenspezifische Verschlüsselung:

Jeder Mandant hat ein eigenes kryptographisches Schlüsselpaar (RSA), das den mandanten-

spezifischen AES-256-Verschlüsselungsschlüssel schützt.

Schlüssel-Vernichtung:

Sichere Löschung des RSA-Schlüsselpaares — der AES-Schlüssel wird damit unzugänglich, alle verschlüsselten E-Mails sind sofort und unwiederbringlich unlesbar.

Effekt:

Alle E-Mails und Daten dieses Mandanten werden sofort und unwiederbringlich unlesbar, selbst wenn gelöschte Datenblöcke auf dem Dateisystem verbleiben sollten.

Mehrschichtige Verschlüsselung:

Die mandantenspezifisch verschlüsselten Daten liegen innerhalb eines LUKS-verschlüsselten Dateisystems (AES-256 in XTS-Modus). Dies bietet eine zusätzliche Sicherheitsebene.

Standard-Verfahren:

Diese Methode entspricht dem Stand der Technik und wird von NIST, BSI und anderen Sicherheitsbehörden für verschlüsselte Systeme empfohlen.

3. Hardware-Entsorgung und Datenträgerlöschung

Bei unserem Betrieb:

- Zusätzliche Infrastruktur-Verschlüsselung auf LUKS-Ebene
- Kryptographische Löschung durch Vernichtung der LUKS-Verschlüsselungsschlüssel bei Serveraustausch
- Dadurch ist eine zusätzliche Sicherheitsebene für alle Mandanten gewährleistet

Bei Hetzner (Hardware-Eigentümer):

Gemäß Hetzner AVV, Anlage 2 (Technische und organisatorische Maßnahmen):

- “Definiertes Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung”
- Bei Dedicated Servern: “Rückstandsfreies Löschen durch eine hardwaregestützte Löschmethode”
- “Physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung”
- Vernichtung erfolgt im Rechenzentrum Falkenstein nach ISO/IEC 21964
- Sichere Transportbehälter bei Datenträger-Transport zwischen Standorten

Verantwortliche:

Die Löschung wird durch autorisierte Administratoren ausgeführt und dokumentiert.

8.3 Löschbestätigung

Die **schriftliche Löschbestätigung** wird auf Anfrage nach Abschluss des Löschvorgangs bereitgestellt. Den konkreten Zeitrahmen regeln die vertraglichen Vereinbarungen (§ 9 AVV). Prozessdetails (Format, Zustellung, Zeitrahmen) werden im Einzelfall mit dem Kunden vereinbart.

Inhalt der Löschbestätigung:

- Datum der Löschung
- Art und Umfang der gelöschten Daten
- Verwendete Löschmethoden
- Bestätigung der vollständigen Löschung
- Unterschrift des verantwortlichen Administrators

Hinweis zu System-Logs:

Die Löschbestätigung umfasst die archivierten E-Mails und Konfigurationsdaten. System-Logs werden im Rahmen der regulären Log-Rotation gelöscht.

White Labeled Benno Cloud:

Reseller erhalten die Löschbestätigung direkt von LWsystems. Endkunden erhalten die Bestätigung über ihren Reseller-Partner.

8.4 Datenportabilität bei Vertragsende

Rechtsgrundlage: § 9 unserer AVV (vertragliche Rückgabe- und Löschpflicht); ergänzend Art. 20 DSGVO (Datenportabilität) sowie — soweit anwendbar — Data Act (Verordnung (EU) 2023/2854)

Unabhängig von der Löschung stellen wir bei Vertragsende alle archivierten E-Mails auf Anforderung in einem **entschlüsselten, portablen** Format zur Verfügung:

Verfügbares Format:

- **EML-Format:**Standard-E-Mail-Format, lesbar mit jedem E-Mail-Client
- Kompatibel mit allen Mail-Clients und gängigen Archivierungslösungen
- Jede E-Mail als separate .eml-Datei für maximale Flexibilität

Bereitstellung:

LWsystems stellt dem Kunden den Download bereit, typischerweise per HTTPS-Download-Link. Bei sehr großen Datenmengen sind mehrteilige Archive oder SFTP-Upload in die Kundeninfrastruktur möglich.

Zeitrahmen:

Der konkrete Zeitrahmen wird im Einzelfall zwischen den Parteien vereinbart. Als Orientierungswert gilt: Bei Datenmengen bis 1 TB typischerweise innerhalb von 20 Werktagen nach Vertragsende. Die verbindlichen Fristen ergeben sich aus der individuellen Vereinbarung — eine allgemeine Zusicherung wird nicht gegeben.

Übergangszeit:

Die Daten werden für einen angemessenen Zeitraum nach Vertragsende vorgehalten, um eine Datenübergabe zu ermöglichen. Die endgültige Löschung erfolgt nach Ablauf des verein-

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

barten Übergangszeitraums gemäß § 9 unserer AVV.

Wichtig: Alle exportierten E-Mails werden entschlüsselt bereitgestellt, damit diese in einem neuen System weiterverwendet werden können.

White Labeled Benno Cloud:

Bereitstellung:

LWsystems stellt dem Reseller-Partner den Download bereit. Dieser gibt die Daten unmittelbar an seinen Endkunden weiter.

Übergangszeit:

Bei White Labeled Benno Cloud werden die Übergangsfristen zwischen Reseller und LWsystems vereinbart.

9. Netzwerksicherheit und Transportverschlüsselung

9.1 Firewall-Architektur

- Host-basierte Paketfilter (LWsystems):
  - Individuell konfiguriert für jeden Server (iptables/nftables)
  - Konfiguration nach dem Prinzip "Default Deny"
  - Nur explizit benötigte Ports geöffnet (SMTP, HTTPS, SSH)
- DDoS-Schutz (Hetzner):
  - Automatische DDoS-Erkennung und -Mitigation (Hetzner setzt auf netzwerkseitige DDoS-Erkennung und -Mitigation durch dedizierte Hardware-Lösungen. Details zu den eingesetzten Systemen sind in Hetzners Sicherheitsdokumentation beschrieben, siehe https://www.hetzner.com/de/unternehmen/ddos-schutz/).
  - Filterung innerhalb von Sekunden nach Angriffserkennung

Hinweis: Eine zentrale Netzwerk-Firewall ist nicht implementiert. Dieser Ansatz vermeidet einen Single Point of Failure und ermöglicht granulare Kontrolle pro Server.

Standard-Firewall-Regeln:

- Port 25 (SMTP): Mailannahme
- Port 443 (HTTPS): Für Web-Interface und API
- Port 22 (SSH): Nur aus LWsystems-Verwaltungsnetz
- Port 21443 (REST API): Benno REST API nur innerhalb der Infrastruktur erreichbar
- Port 21543 (REST API): REST Import Schnittstelle, per API Token gesichert
- Alle anderen Ports: Geschlossen

9.2 DDoS-Schutz

Dauerhaft aktive DDoS-Erkennung:

- Netzwerk-Ebene: Hetzner bietet automatische DDoS-Erkennung und -Mitigation (Hetzner setzt auf dedizierte Hardware-Lösungen. Details zu den eingesetzten Systemen sind in Hetzners Sicherheitsdokumentation beschrieben, siehe https://www.hetzner.com/de/unternehmen/ddos-schutz/).
- Automatische Filterung innerhalb von Sekunden nach Angriffserkennung

Maßnahmen bei DDoS-Angriffen:

- Automatische Mitigation durch Hetzner (SYN Floods, UDP Floods, DNS Reflection)
- Bei extremen Angriffen (> 10 Gbit/s): Temporäres Blackholing durch Hetzner zum Schutz der Infrastruktur
- Monitoring und Alerting durch LWsystems

9.3 Monitoring und Alerting

Monitoring und Alerting

- System-Monitoring: Überwachung von Systemressourcen, Services und Verfügbarkeit
- Automatisches Blocking bei erkannten Brute-Force-Angriffen
- Benachrichtigung bei kritischen Events an Administrator-Team

9.4 TLS/SSL-Konfiguration

Web-Interface und API:

- **Protokoll**: TLS in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2). TLS 1.0 und 1.1 sind deaktiviert.
- **Cipher Suites**: Es werden ausschließlich Cipher Suites eingesetzt, die den aktuellen BSI-Empfehlungen (TR-02102-2) entsprechen und Perfect Forward Secrecy (PFS) unterstützen.
- **Perfect Forward Secrecy**: Ja (ECDHE)
- **HSTS**: Aktiviert (HTTP Strict Transport Security)
- **Zertifikate**: Öffentlich vertrauenswürdige TLS-Zertifikate (Let's Encrypt oder kundenspezifische Zertifikate)

SMTP (E-Mail-Empfang):

- **STARTTLS**: Verpflichtend für eingehende Verbindungen
- **TLS-Version**: TLS in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2). TLS 1.0 und 1.1 sind deaktiviert.
- **Cipher Suites**: Es werden ausschließlich Cipher Suites eingesetzt, die den aktuellen BSI-Empfehlungen (TR-02102-2) entsprechen und Perfect Forward Secrecy (PFS) un-

terstützen.

TLS-Verhandlung mit Microsoft 365 bzw. Mailzulieferung aus anderen Quellen:

Wenn Microsoft 365 Journal-Mails bzw. andere Quellen E-Mails zu uns senden:

1. Sendende Seite sendet “ClientHello” mit Liste unterstützter TLS-Versionen
2. Unser Server wählt die höchste gemeinsam unterstützte Version
3. Cipher Suite wird nach Sicherheit und Performance ausgewählt

Warum TLS 1.2 als Minimum?

- Microsoft 365 hat TLS 1.0/1.1 seit Oktober 2020 deaktiviert
- BSI-Empfehlung: Mindestens TLS 1.2
- Bekannte Schwachstellen in TLS 1.0/1.1 (BEAST, POODLE, Sweet32)
- DSGVO-Konformität: “Stand der Technik”

10. Mitarbeiterverpflichtungen und Schulungen

10.1 Verpflichtung auf das Datengeheimnis

Alle Mitarbeiter werden vor Tätigkeitsbeginn verpflichtet:

- **DSGVO**: Verpflichtung auf Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b DSGVO
- **§ 203 StGB**: Zusätzliche Verpflichtung auf strafrechtliche Schweigepflicht für Projekte mit Berufsgeheimnisträgern
- **Fortdauer**: Die Verpflichtung besteht zeitlich unbegrenzt fort, auch nach Beendigung des Arbeitsverhältnisses

Dokumentation:

- Schriftliche Verpflichtungserklärungen mit Unterschrift
- Regelmäßige Sensibilisierung und Schulung — Frequenz und Einzelheiten sind in den internen Prozessdokumenten geregelt
- Nachweis für Audits verfügbar

10.2 Datenschutzschulungen

Regelmäßige Schulungen:

- **Frequenz**: Regelmäßig gemäß interner Prozessdokumente
  - **Inhalte**:
    - DSGVO-Grundlagen und Pflichten als Auftragsverarbeiter
    - Technische und organisatorische Maßnahmen
    - Umgang mit Sicherheitsvorfällen

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

- § 203 StGB für Projekte mit Berufsgeheimnisträgern
- Praktische Fallbeispiele

Zielgruppen:

- Alle Mitarbeiter: DSGVO-Grundlagen
- Administratoren: Erweiterte Schulung zu TOMs und Incident Response
- Entwickler: Privacy by Design, sichere Entwicklung

10.3 § 203 StGB - Besondere Schweigepflicht

Alle Mitarbeiter mit potenziellem Datenzugriff werden regelmäßig — mindestens jährlich — zu § 203 StGB geschult. Neue Mitarbeiter werden vor Tätigkeitsbeginn geschult.

Die Schulung umfasst:

- Rechtliche Grundlagen des § 203 StGB (Verletzung von Privatgeheimnissen)
- Status als “mitwirkende Personen” (§ 203 Abs. 3 StGB)
- Strafbarkeit bei unbefugter Offenbarung durch mitwirkende Personen (§ 203 Abs. 1 i.V.m. Abs. 3 Satz 2 StGB)
- Definition “fremde Geheimnisse” (Patientendaten, Mandantendaten, etc.)
- Verbotene Handlungen und erlaubte Zugriffe
- Praktische Fallbeispiele und Diskussion

Dokumentation:

- Teilnehmerlisten mit Unterschrift
- Schriftliche Verpflichtungserklärungen mit explizitem Hinweis auf § 203 StGB
- Nachweis für Kunden und Aufsichtsbehörden verfügbar

10.4 Sicherheitsbewusstsein

Kontinuierliche Sensibilisierung:

- Phishing-Simulationen (fortlaufend)
- Security Awareness-Newsletter
- Meldepflicht für verdächtige Vorgänge
- Clear-Desk-Policy
- Passwort-Management-Training

11. Audits und Zertifizierungen

11.1 Interne Audits

Regelmäßige Überprüfungen:

LWsystems führt regelmäßige interne Überprüfungen der technischen und organisatorischen Maßnahmen durch (Art. 32 Abs. 1 lit. d DSGVO). Frequenz, Umfang und Durchführung sind in den internen Prozessdokumenten geregelt.

Audit-Bereiche:

Die Audit-Bereiche, Methodik, Verantwortlichkeiten und Dokumentation sind in den internen Prozessdokumenten geregelt. Die Prüfung umfasst alle datenschutzrelevanten technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 lit. d DSGVO.

11.2 Kontrollrechte des Auftraggebers

Nachweis durch Dokumentation:

- Aktuelle Testate und Audit-Berichte
- Technische und organisatorische Maßnahmen (TOMs)
- Zertifizierungen (ISO 27001:2022 von Hetzner)
- Datenschutzkonzepte
- AVV mit Unterauftragnehmern

Anforderung:

- datenschutz@lw-systems.de

Bereitstellung:

- Innerhalb eines angemessenen Zeitraums nach Anforderung

Vor-Ort-Audits:

- Maximal 1 Audit pro Kalenderjahr (sofern nicht durch Datenpanne oder behördliche Anordnung begründet)
- Mindestens 2 Wochen Vorlauf
- Während üblicher Geschäftszeiten
- Durchführung ohne Störung des Betriebsablaufs
- Wahrung von Vertraulichkeitsinteressen
- Beschränkt auf die Verarbeitung der personenbezogenen Daten des Kunden

Die vollständigen Bedingungen und Voraussetzungen sind in § 7 unserer AVV geregelt.

Aufwendungsersatz / Ersatz von Aufwendungen:

- Bei Audits, die nicht durch unseren Verstoß begründet sind, können wir den Ersatz von Aufwendungen verlangen
- Ohne Aufwendungsersatz bei festgestellten Verstößen gegen die AVV

White Labeled Benno Cloud

Für Reseller-Partner:

- Reseller haben die gleichen Kontrollrechte wie Direktkunden und können diese auch im Auftrag ihrer Endkunden ausüben.

Für Endkunden von Resellern:

- Kontrollrechte werden über den Reseller ausgeübt. Der Reseller kann im Auftrag des Endkunden Audits bei LWsystems durchführen oder Nachweise anfordern.

11.3 Zertifizierungen

Hetzner Online GmbH (Rechenzentren):

- **ISO 27001:2022** (Informationssicherheits-Management-System — ISMS)
  Aktuelle Zertifizierung: https://www.hetzner.com/de/unternehmen/zertifizierung
- Geltungsbereich: Rechenzentren Nürnberg und Falkenstein
- Physische Sicherheit, Zutrittskontrolle, Umgebungsüberwachung
- Netzwerksicherheit, Hardware-Management
- Incident Management, Business Continuity
- Datenschutz-Informationssicherheits-Management-System (DIMS)
- Regelmäßige externe Überprüfung der TOMs
- Zertifikat verfügbar unter:
  https://www.hetzner.com/de/unternehmen/zertifizierung

LWsystems:

- **Auftragsverarbeitung auf Grundlage eines vollständigen AVV** nach Art. 28 DSGVO mit dokumentierten TOMs nach Art. 32 DSGVO
- **Regelmäßige interne Audits** der Sicherheitsmaßnahmen
- **Regelmäßige Überprüfung** der technischen und organisatorischen Maßnahmen — Frequenz und Methodik in den internen Prozessdokumenten geregelt

11.4 Zusammenarbeit mit Aufsichtsbehörden

Bei Prüfungen durch Datenschutz-Aufsichtsbehörden:

- LWsystems kooperiert mit der zuständigen Aufsichtsbehörde im gesetzlich gebotenen Umfang
- Alle angeforderten Informationen werden bereitgestellt
- Zugang zu Systemen wird (soweit datenschutzrechtlich zulässig) gewährt
- Der Kunde wird über die Prüfung informiert

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

White Labeled Benno Cloud:

LWsystems unterstützt den Reseller bei der Erfüllung seiner Auskunftspflichten gegenüber Aufsichtsbehörden. Die Informationskette verläuft über den Reseller.

11.5 Kontakt für Audit-Anfragen

Benno Cloud Enterprise (Direktkunden):

- **E-Mail:** datenschutz@lw-systems.de
- **Telefon:** +49 5403 88017-0

White Labeled Benno Cloud (Reseller):

- **E-Mail:** datenschutz@lw-systems.de
- **Telefon:** +49 5403 88017-0

White Labeled Benno Cloud (Endkunden):

- Kontakt über den Reseller-Partner

Hinweis zur Datenschutzverantwortung: Die datenschutzrechtliche Verantwortung bei LW-systems liegt bei der Geschäftsführung. Für datenschutzrechtliche Anfragen steht datenschutz@lw-systems.de zur Verfügung.

12. Häufig gestellte Fragen (FAQ)

12.1 Verschlüsselung

Q: Warum zweifache Verschlüsselung?

A: Wir setzen auf ein **Defense-in-Depth-Konzept** mit zwei unabhängigen Verschlüsselungsebenen:

1. **Mandantenspezifische Verschlüsselung:** Jeder Mandant hat sein eigenes RSA-Schlüsselpaar. Die archivierten E-Mails werden AES-256-verschlüsselt. Selbst wenn jemand Zugriff auf die Infrastruktur hätte, könnte er keine E-Mails lesen.
2. **Infrastruktur-Verschlüsselung (LUKS):** Die gesamte Hardware ist vollverschlüsselt. Selbst bei physischem Diebstahl bleiben alle Daten geschützt.

Vorteil: Maximale Sicherheit durch Redundanz. Selbst bei Kompromittierung einer Ebene bleiben die Daten geschützt.

Q: Sind meine E-Mails verschlüsselt gespeichert?

A: Ja. Alle E-Mails werden auf vollverschlüsselten Dateisystemen (LUKS mit AES-256) gespeichert. Zusätzlich werden die E-Mails selbst mandanten-spezifisch mit AES-256 verschlüsselt.

Q: Wer hat die Verschlüsselungsschlüssel?

A: Standardmäßig befinden sich die Schlüssel in unserer verschlüsselten Infrastruktur. Auf Wunsch können Kunden die Schlüssel zur sicheren Verwahrung erhalten. Bei Vertragsende werden alle Daten entschlüsselt und portabel bereitgestellt.

Q: Warum verwendet ihr kein HSM (Hardware-Sicherheitsmodul)?

A: Für E-Mail-Archivierung bietet LUKS-Verschlüsselung ein angemessenes Sicherheitsniveau, das DSGVO- und BSI-Anforderungen erfüllt. HSM ist primär für Payment-Systeme, Zertifizierungsstellen oder Behörden mit höchsten Sicherheitsstufen relevant und würde erhebliche Mehrkosten ohne nennenswerten Sicherheitsgewinn verursachen.

Q: Ist die Übertragung von Microsoft 365 und anderen Quellen zu euch verschlüsselt?

A: Ja. Der Transport erfolgt via SMTP mit TLS Verschlüsselung. TLS wird in einer dem Stand der Technik entsprechenden Version (gemäß BSI TR-02102-2) verwendet. TLS 1.0 und 1.1 sind deaktiviert (bekannte Sicherheitslücken).

12.2 Zugriff und Kontrolle

Q: Können LWsystems-Mitarbeiter meine E-Mails lesen?

A: Technisch ist ein Zugriff durch autorisierte Administratoren möglich – dies ist für Betrieb und Support unverzichtbar. Rechtlich und organisatorisch ist dies durch mehrere Ebenen abgesichert: Verpflichtung auf Datengeheimnis, § 203 StGB, strafrechtliche Konsequenzen (§ 202a StGB), Protokollierung. Administratoren greifen nur für Systemadministration oder auf ausdrückliche Anfrage des Kunden zu, nicht zur inhaltlichen Einsichtnahme.

Q: Wo liegen meine Daten?

A: Ausschließlich in Deutschland (Hetzner-Rechenzentren in Nürnberg und Falkenstein). Keine Verarbeitung außerhalb der EU.

Q: Kann ich selbst Audits durchführen?

A: Ja. Gemäß § 7 unserer AVV haben Kunden Kontrollrechte. Maximal 1 Audit pro Jahr (ohne besonderen Anlass), mit 2 Wochen Vorlauf. Auf Anfrage werden auch Dokumentationen und Audit-Berichte zur Verfügung gestellt.

12.3 Datenschutz und Compliance

Q: Ist der Service DSGVO-konform?

A: LWsystems erbringt seine Leistungen als Auftragsverarbeiter auf Grundlage eines vollständigen AVV nach Art. 28 DSGVO und stellt die vertraglichen und technischen Grundlagen für den DSGVO-konformen Einsatz durch den Kunden bereit: vollständiger Auftragsverarbeitungsvertrag (Art. 28 DSGVO), implementierte TOMs (Art. 32 DSGVO) und Unterstützung bei Betroffenenrechten und Meldepflichten.
Die datenschutzrechtliche Verantwortung für die Rechtmäßigkeit der Verarbeitung verbleibt

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

beim Kunden als Verantwortlichem (Art. 4 Nr. 7 i.V.m. Art. 24 DSGVO).

Q: Unterstützt der Service GoBD-konforme Archivierung?

A: Ja, in erheblichem Umfang. Als technischer Betreiber übernimmt LWsystems den weitaus größten Teil der GoBD-Umsetzungsleistungen — insbesondere Unveränderbarkeit im Sinne der GoBD (d.h. Änderungen sind erkennbar und nachvollziehbar), Vollständigkeit, Nachvollziehbarkeit, Revisionssicherheit und maschinelle Auswertbarkeit sowie die Bereitstellung der Verfahrensdokumentation (Systemteil).
Die steuerrechtliche Gesamtverantwortung verbleibt gemäß GoBD Rz. 21 beim Kunden als Steuerpflichtigem — auch bei vollständiger technischer Auslagerung. Kundenseitig sind einige organisatorische Maßnahmen erforderlich (u.a. E-Mail-Zuführung einrichten, Verfahrensdokumentation unterzeichnen, interne Regelungen treffen). LWsystems unterstützt und berät dabei. Details siehe Kapitel 5.4.

Q: Sind eure Mitarbeiter auf § 203 StGB verpflichtet?

A: Ja. Alle Mitarbeiter mit potenziellem Datenzugriff sind explizit auf die strafrechtliche Schweigepflicht nach § 203 StGB verpflichtet. Alle Mitarbeiter mit potenziellem Datenzugriff werden regelmäßig – mindestens jährlich – geschult. Neue Mitarbeiter werden vor Tätigkeitsbeginn geschult. Dies gilt insbesondere für Projekte im Gesundheitswesen oder mit Rechtsanwälten/Steuerberatern.

Q: Können einzelne E-Mails während der Vertragslaufzeit gelöscht werden (z.B. aufgrund einer DSGVO-Löschanforderung)?

A: Ja. Löschanforderungen für einzelne E-Mails — etwa aufgrund von Betroffenenrechten nach Art. 17 DSGVO — werden auf schriftliche Weisung des Kunden von LWsystems ausgeführt und intern protokolliert. Eine Self-Service-Funktion für Kunden ist in einer zukünftigen Version der Anwendung geplant.

Q: Kann ich mit dem Audit-Log meine Mitarbeiter überwachen?

A: Das Audit-Log protokolliert Suchabfragen im Archiv und dient primär der Nachvollziehbarkeit von Archivzugriffen für **Compliance-Zwecke**. Es erfasst gegenwärtig Suchbegriffe, Filter und Zeitpunkte — nicht jedoch, welche E-Mails konkret geöffnet oder heruntergeladen wurden. Eine Erweiterung ist geplant.

Eine permanente, anlasslose Überwachung von Mitarbeiterzugriffen ist in Deutschland **nur unter engen Voraussetzungen zulässig**:

- Rechtsgrundlage vorhanden (z.B. berechtigtes Interesse)
- Verhältnismäßigkeitsprüfung durchgeführt
- Mitarbeiter informiert
- Ggf. Betriebsvereinbarung geschlossen

Wir empfehlen, das Audit-Log nur für **konkrete Compliance-Anforderungen** (z.B. § 203

StGB im Gesundheitswesen) oder **bei Verdacht auf Datenmissbrauch** zu nutzen.

Bei Fragen zur rechtssicheren Implementierung beraten wir gerne oder vermitteln den Kontakt zu spezialisierten Datenschutzexperten.

12.4 Subunternehmer

Q: Welche Subunternehmer setzt ihr ein?

A: Aktuell nur Hetzner Online GmbH für die Bereitstellung der Server-Infrastruktur (Rechenzentren in Deutschland, ISO 27001:2022-zertifiziert). Keine weiteren Subunternehmer. Keine Drittland-Übermittlungen.

Q: Was passiert, wenn ihr weitere Subunternehmer einbindet?

A: Kunden werden mindestens 2 Wochen vorab informiert. Kunden haben ein Widerspruchsrecht. Wir schließen mit jedem Subunternehmer einen vollständigen AVV ab mit mindestens denselben Verpflichtungen wie in unserem Vertrag mit dem Kunden.

12.5 Sicherheitsvorfälle

Q: Wie schnell werdet ihr mich bei einem Sicherheitsvorfall informieren?

A: Unverzüglich nach Kenntniserlangung, ohne schuldhaftes Zögern — entsprechend unserer Pflicht aus § 8 unserer AVV.

Q: Was umfasst die Meldung?

A: Art der Verletzung, Kategorien und Anzahl betroffener Personen/Daten, Kontaktdaten unseres Datenschutzverantwortlichen, Folgenabschätzung, ergriffene und vorgeschlagene Gegenmaßnahmen.

Q: Gilt das auch für Sicherheitsvorfälle bei Hetzner?

A: Ja. Hetzner ist vertraglich verpflichtet, uns unverzüglich zu informieren. Die Information wird unverzüglich an Kunden weitergeleitet.

12.6 Vertragsende und Hardware-Entsorgung

Q: Was passiert mit meinen Daten nach Vertragsende?

A: Alle Daten werden vollständig und unwiederbringlich gelöscht (§ 9 unserer AVV). Auf Anfrage stellen wir archivierten E-Mails vor der Löschung in entschlüsseltem, portablem Format (.eml) zur Verfügung. Auf Wunsch wird eine schriftliche Löschbestätigung ausgestellt. Die konkreten Abläufe und Fristen werden im Einzelfall vereinbart.

Q: Wie lange dauert die Datenbereitstellung?

A: In der Regel innerhalb von 20 Werktagen nach Vertragsende (bei Datenmengen bis 1 TB). Bei größeren Datenmengen ist eine gesonderte Abstimmung erforderlich. Die verbindliche Frist wird im Einzelfall vereinbart.

Q: Kann ich die Daten auch während der Vertragslaufzeit exportieren?

A: Ja, jederzeit auf Anfrage. Export-Format: .eml

Q: Was passiert mit defekten oder ausgetauschten Festplatten bei Hetzner?

A: Hetzner hat in seiner AVV verbindlich festgelegt:

1. **Sichere Löschung:** Rückstandsfreies Löschen durch hardwaregestützte Löschmethoden
2. **Physische Vernichtung:** Bei nicht erfolgreicher Datenlöschung erfolgt physische Zerstörung nach ISO/IEC 21964
3. **Kontrollierte Vernichtung:** Erfolgt im Rechenzentrum Falkenstein mit sicheren Transportbehältern

Wichtig: Da unsere gesamte Infrastruktur LUKS-verschlüsselt ist, sind die Daten selbst bei physischem Diebstahl oder unsachgemäßer Entsorgung ohne die Verschlüsselungsschlüssel nicht lesbar.

12.7 Technische Fragen

Q: Wie wird die Verfügbarkeit sichergestellt?

A: 3-fach redundante Infrastruktur, automatisches Failover, redundante Stromversorgung (USV + NEA), redundante Kühlung, redundante Netzwerkanbindung. (Verfügbarkeit gemäß Annex A – SLA unserer AGB. Rechtsverbindlich sind ausschließlich die im SLA definierten Parameter).

Q: Gibt es DDoS-Schutz?

A: Ja, dauerhaft aktive DDoS-Erkennung auf Netzwerk-Ebene (Hetzner) und Anwendungs-Ebene (Rate-Limiting).

Q: Werden Backups erstellt?

A: Nein, bei Benno Cloud Enterprise werden keine separaten Backups erstellt. Dies ist bewusst so konzipiert und in der Leistungsbeschreibung dokumentiert.

Grund: Hochverfügbare Architektur statt Backups

Statt eines traditionellen Backup-Konzepts setzen wir auf eine **3-fach redundante, geo-verteilte Architektur**:

- **3 physisch separate Server-Nodes** in verschiedenen Rechenzentrumsabschnitten
- **Automatische Replikation** im 15-Minuten-Intervall auf alle drei Nodes
- **Automatisches Failover**: Bei Ausfall eines Nodes übernehmen die verbleibenden Nodes ohne Datenverlust
- **Geo-Redundanz**: Die Nodes befinden sich an unterschiedlichen Rechenzentrumsstandorten des Anbieters (Nürnberg, Falkenstein)

- **Standort:** Alle drei redundanten Nodes befinden sich ausschließlich in Deutschland (Nürnberg/Falkenstein). Eine Datenverarbeitung oder -speicherung außerhalb Deutschlands findet nicht statt.

Vorteile gegenüber klassischen Backups:

Aspekt	Klassisches Backup	Unsere Redundanz
Datenverlust-Risiko	Bis zu 24h (je nach Backup-Frequenz)	Maximal 15 Minuten (Replikationsintervall)
Recovery Time	Stunden bis Tage	Sekunden (automatisch)
Aktualität	Veraltet (letztes Backup)	Immer aktuell
Hardware-Ausfall	Service-Unterbrechung während Restore	Kein Ausfall dank Failover

Schutz vor:

- Hardware-Ausfall (Server, Festplatten)
- Datenverlust durch Defekte
- Ausfall einzelner Rechenzentrumsabschnitte bzw. -standorte
- Stromausfall einzelner Systeme

Wann sind zusätzliche Backups sinnvoll?

Die redundante Architektur schützt gegen technische Ausfälle. Für folgende Szenarien können eigene Backups in Betracht gezogen werden:

- Compliance-Anforderungen für zusätzliche Offline-Kopien
- Schutz vor Ransomware mit Admin-Zugriff

Hierfür bieten wir auf Nachfrage jederzeit gesonderte Optionen an.

Q: Was passiert, wenn zwei Nodes gleichzeitig ausfallen?

A: In diesem Fall übernimmt der 3. Node alle Funktionen. Ein gleichzeitiger Ausfall von zwei Nodes ist darüber hinaus extrem unwahrscheinlich, da:

- Die Nodes in verschiedenen Stromkreisen und Kühlzonen stehen
- Unabhängige Hardware verwendet wird
- Wartungsarbeiten zeitlich versetzt durchgeführt werden

Q: Kann ich den Service in mein SSO integrieren?

A: Ja. Wir unterstützen OAuth 2.0. Integration mit dem Identity Provider des Kunden ist möglich.

Q: Existiert eine zentrale Netzwerk-Firewall vor dem Cluster?

A: Nein. Jeder Server im Cluster hat einen eigenen, restriktiv konfigurierten Paketfilter (ipta-

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de

bles/nftables). Diese Host-basierten Firewalls arbeiten nach dem Prinzip "Default Deny" – nur explizit benötigte Ports sind geöffnet. Zusätzlich bietet Hetzner einen automatisierten DDoS-Schutz auf Netzwerkebene.

Dieser Ansatz hat Vorteile:

- Keine Single Point of Failure (zentrale Firewall fällt aus = alle Server offline)
- Bessere Performance (keine zusätzliche Latenz durch zentrale Appliance)
- Granulare Kontrolle pro Server

Für die meisten Anwendungsfälle ist eine zentrale Firewall nicht erforderlich, da der kombinierte Schutz aus Host-Firewalls, DDoS-Mitigation und restriktiven Netzwerkregeln ein hohes Sicherheitsniveau bietet.

12.8 Support und Verfügbarkeit

Q: Wie erreiche ich den Support?

A:

- E-Mail: support@benno-mailarchiv.de
- Telefon: +49 5403 88017-80 (Mo-Fr 9-17 Uhr)
- Kritische Vorfälle: Für kritische Vorfälle außerhalb der Supportzeiten steht ein Notfallkontakt zur Verfügung, der individuell im Servicevertrag vereinbart wird.

Q: Gibt es geplante Wartungsfenster?

A: Geplante Wartungsarbeiten werden **im Voraus mit dem Kunden vereinbart**. Gemäß unseres Service Level Agreement (SLA, Annex A unserer AGB) werden vereinbarte Wartungszeiten nicht auf die Verfügbarkeit angerechnet.

Planung: Wartungsfenster werden typischerweise außerhalb der Hauptgeschäftszeiten gelegt (z.B. nachts oder am Wochenende).

Redundanz-Vorteil: Dank der 3-fach redundanten Architektur können viele Wartungsarbeiten ohne Service-Unterbrechung durchgeführt werden.

Notfall-Wartung: Bei unvorhergesehen erforderlichen Wartungsarbeiten (z.B. kritische Sicherheitsupdates) werden Kunden schnellstmöglich informiert.

Verfügbarkeitszusage: 99,3% während der vereinbarten Verfügbarkeitszeit (Mo-So, 6:00-20:00 Uhr) gemäß SLA unserer AGB.

12.9 White Labeled Benno Cloud

Q: Können Reseller Endkunden mit unterschiedlichen Mailsystemen betreiben?

A: Ja, uneingeschränkt. Jeder Endkunde eines Resellers wird als eigenständiger Mandant in Benno Cloud betrieben — vollständig technisch von allen anderen Mandanten getrennt, mit eigenem verschlüsseltem Archiv und eigener Benutzerverwaltung. Die Art des Mailsystems des Endkunden (Microsoft 365, gehosteter Mailservice, eigener Mailserver u.a.) ist dabei irre-

levant: Benno Cloud unterstützt alle gängigen Zuführungswege (Journaling, SMTP, REST-API). Ein Reseller kann daher beliebig viele Endkunden mit technisch unterschiedlichen Mailumgebungen in seinem Bestand betreiben.

13. Kontakt

Allgemeine Anfragen

LWsystems GmbH & Co. KG
Tegelerweg 11
49186 Bad Iburg
Deutschland

Telefon: +49 5403 88017-0
E-Mail: info@lw-systems.de
Web: https://www.lw-systems.de

Datenschutzverantwortlicher

Name: Ansgar Licher
Funktion: Geschäftsführung

Telefon: +49 5403 88017-0
E-Mail: datenschutz@lw-systems.de

Sicherheitsvorfälle

Security Incident Response Team
E-Mail: admin@lw-systems.de
Telefon: +49 5403 88017-0

Impressum

LWsystems GmbH & Co. KG

Anschrift:
Tegelerweg 11
49186 Bad Iburg
Deutschland

Vertretungsberechtigte Geschäftsführer:
Ansgar Licher, Martin Werthmöller

Registergericht:
Bad Iburg

Registernummer:
HRB 111163

Umsatzsteuer-Identifikationsnummer:
Umsatzsteuer-Identifikationsnummer gemäß §27 a Umsatzsteuergesetz: USt-IdNr.
DE244573220

Verantwortlich für den Inhalt nach § 55 Abs. 2 RStV:
Ansgar Licher

Kontakt:
Telefon: +49 5403 88017-0
E-Mail: info@lw-systems.de
Website: www.lw-systems.de

Vielen Dank für das Vertrauen in LWsystems und Benno Cloud Enterprise!

Wir legen größten Wert auf Sicherheit, Datenschutz und Transparenz. Bei weiteren Fragen steht unser Team gerne zur Verfügung.

14. Versionshistorie

Version	Datum	Änderungen
1.0	Dezember 2025	Entwurfsversion
1.1	Januar 2026	Div. Detailpräzisierungen
1.2	Februar 2026	Präzisierungen nach juristischer Tiefenprüfung
1.3	Februar 2026	Präzisierungen nach juristischer Tiefenprüfung
1.4	Februar 2026	Executive Summary ergänzt
1.5	Februar 2026	Weitere Präzisierungen nach juristischer Tiefenprüfung
1.6	März 2026	Finalisierung und Pflege weiterer Präzisierungen
1.7	13. März 2026	Pre-Finalisierung, Abstraktion best. Abschnitte mit Verweis auf die internen Prozessdokumente, einzelne Passagen pragmatischer dargestellt.
1.8	16. März 2026	Pflege weiterer Präzisierungen
1.9	16. März 2026	Pflege weiterer Präzisierungen
2.0	17. März 2026	Finalisierung und Pflege weiterer Präzisierungen
2,1	18. März 2026	Finalisierung und Pflege weiterer Präzisierungen
2.2	26. März 2026	Finalisierung, Vorbereitung und Durchführung anwaltlicher Prüfung
2.3	30. April 2026	Fertigstellung des Dokuments in veröffentlichungsfähiger Form nach vorangegangener anwaltlicher Prüfung Erste öffentliche Version

LWsystems GmbH & Co. KG >> Tegelerweg 11 >> 49186 Bad Iburg >> Telefon 05403/88017-0 >> E-Mail info@benno-mailarchiv.de >> Internet www.benno-mailarchiv.de