Hersteller-Systembeschreibung Neretha

Stand 2026.10-2 vom 29.10.2026

Diese Beschreibung ist die technische Systemdokumentation des Herstellers. Sie ersetzt nicht deine eigene Verfahrensdokumentation, sondern ist deren Anlage (Kapitel 7 „Eingesetzte Hard- und Software“). Sie beschreibt, was die Software tut – nicht, wie dein Betrieb organisiert ist.

Keine Zertifizierung. Für Neretha liegt kein Softwaretestat (z. B. nach IDW PS 880) und keine GoBD-Zertifizierung vor. Eine solche Zertifizierung durch die Finanzverwaltung gibt es nicht (GoBD Rz. 180). Ordnungsmäßigkeit entsteht erst aus Software und Ablauf im Betrieb zusammen.

1. Produkt und Hersteller

Produkt: Neretha Büro und Buchhaltung (Web-Anwendung)

Hersteller und Betreiber: Neretha Services (Angaben siehe Impressum)

Betriebsart (diese Beschreibung): Server-Betrieb: Software als Dienst, Nutzung im Browser, Server in Deutschland

Weitere Betriebsart: Lokaler Betrieb auf eigenem Rechner (Mac/Linux) auf Anfrage – siehe Abschnitt 2a

Mandantentrennung: Jede Firma ist ein eigener Mandant; Abfragen sind serverseitig auf die Firma begrenzt

Stand der Beschreibung: 2026.10-2 vom 29.10.2026

2. Betrieb und Standort

1. Server bei Hetzner Online GmbH, Rechenzentrum Falkenstein (Deutschland). Das Rechenzentrum ist nach ISO/IEC 27001 zertifiziert (laut Anbieter); die Zertifizierung betrifft den Anbieter, nicht Neretha.
2. Verbindung durchgehend verschlüsselt (HTTPS/TLS). Datenbank: SQLite auf dem Server, Dateien (Belege) im Dateisystem des Servers.
3. Wartungszugang des Betreibers nur per SSH-Schlüssel. Zugriff des Betreibers auf Kundendaten nur zur Wartung und Fehlerbehebung nach dem Vertrag zur Auftragsverarbeitung (AVV).
4. Updates werden zentral eingespielt. Vor jedem Update wird die Datenbank gesichert.

2a. Lokaler Betrieb (auf Anfrage)

Neretha kann auf Anfrage auch lokal auf einem eigenen Rechner laufen (heute Mac oder Linux; Windows ist noch nicht geprüft). Dann gilt Abschnitt 2 nicht: Datenbank und Belegarchiv liegen in einem Datenordner, den das Unternehmen selbst wählt (z. B. interne Platte, USB-Platte oder NAS). Der Hersteller hat keinen Zugriff und keine Kopie. Sicherung, Verschlüsselung, Zugriffsschutz des Rechners und Aufbewahrung über die gesamte Frist liegen vollständig beim Unternehmen; das ist in der eigenen Verfahrensdokumentation zu beschreiben. Die Funktionen aus den Abschnitten 3 bis 9 arbeiten in beiden Betriebsarten gleich.

Apps für Mac, Windows, Linux, iOS und Android sind geplant und heute nicht verfügbar. Im Browser lässt sich die Web-App auf dem Startbildschirm ablegen (ohne Offline-Datenhaltung).

3. Belege erfassen und archivieren

1. Eingang: Upload im Browser, E-Mail-Eingangsadresse, Belegfoto (optional, wenn freigeschaltet) und Erfassung von Ausgangsrechnungen in Neretha.
2. Beim Archivieren berechnet Neretha einen SHA-256-Fingerabdruck der Datei und speichert die Datei neben vorhandenen Dateien (anhängend, keine Überschreibung).
3. E-Rechnungen (XRechnung, ZUGFeRD): Die strukturierte XML-Datei wird als Original aufbewahrt; die Sichtdarstellung ist nur eine Lesehilfe.
4. Korrekturen archivierter Belege nur über Storno und Nachfolgebeleg; der Ursprungsbeleg bleibt erhalten und verknüpft.

5. Eine Integritätsprüfung vergleicht gespeicherte Dateien mit ihren Fingerabdrücken und zeigt Abweichungen an.

4. Ausgangsrechnungen und Nummernkreise

1. Rechnungsnummern werden fortlaufend und automatisch vergeben; Lücken im Nummernkreis zeigt die App an.
2. E-Rechnungen werden als XRechnung bzw. ZUGFeRD erzeugt. Der Hersteller prüft die Erzeugung bei jeder Programmänderung automatisiert mit dem offiziellen KoSIT-Prüfwerkzeug.
3. Versendete Rechnungen werden archiviert; eine Änderung ist nur per Storno-Rechnung möglich.

5. Unveränderbarkeit und Protokollierung

1. Audit-Log: wichtige Aktionen (Archivieren, Löschen, Sperren, Entsperren, Einfrieren, Exporte) werden mit Zeit, Person und Aktion protokolliert. Die Anwendung bietet keine Funktion zum Ändern oder Löschen von Einträgen.
2. Monatsabschluss mit Periodensperre; Entsperren nur mit Begründung, die im Audit-Log steht.
3. Verfahrensdokumentation: Eingefrorene Versionen werden als unveränderlicher Text gespeichert und mit SHA-256 ausgewiesen; Änderungen nur über eine neue Version.
4. Optional Zweitbestätigung per Passphrase für kritische Aktionen.
5. Grenze: Es gibt keine WORM-Speicherung (Write Once Read Many). Wer Administratorzugriff auf den Server hat, könnte Daten technisch verändern; Fingerabdrücke und Sicherungen machen das erkennbar, verhindern es aber nicht.

6. Aufbewahrung und Löschschutz

1. Archivierte Unterlagen sind standardmäßig 10 Jahre ab Ende des Kalenderjahres gegen Löschen gesperrt (einstellbar bis 30 Jahre, nicht kürzer).
2. Gesetzlich gelten 10 Jahre für Bücher und Organisationsunterlagen, 8 Jahre für Buchungsbelege und Rechnungen (seit 01.01.2025) und 6 Jahre für Handels- und Geschäftsbriefe (§ 147 AO, § 14b UStG). Der Löschschutz liegt bewusst auf der sicheren Seite.
3. Neretha löscht nie automatisch. Nach Fristablauf löscht nur ein berechtigter Nutzer von Hand mit Begründung; die Löschung wird protokolliert.
4. Nach Vertragsende werden die Daten exportiert bereitgestellt (mindestens 30 Tage) und danach gelöscht. Die Aufbewahrung über das Vertragsende hinaus liegt beim Kunden – deshalb vorher den vollständigen Export sichern.

7. Datensicherung

1. Sicherung der Datenbank vor jedem Update sowie tägliche verschlüsselte Sicherung (AES-256), Aufbewahrung höchstens 90 Tage, zusätzliche verschlüsselte Kopie außerhalb des Servers in Deutschland.
2. Eine Voll-Rücksicherung wurde am 21.10.2026 erfolgreich erprobt.
3. Die Sicherungen des Betreibers dienen der Verfügbarkeit, nicht der langjährigen Aufbewahrung. Für die 10-jährige Aufbewahrung braucht der Kunde eigene Exporte (Prüfungs-ZIP) an einem eigenen Ort.
4. Im lokalen Betrieb (Abschnitt 2a) gibt es keine Sicherung durch den Hersteller: Das Unternehmen sichert den Datenordner selbst, verschlüsselt, auf ein zweites Medium und außer Haus, und testet die Wiederherstellung.

8. Zugriff und Rollen

Inhaber: alles, darunter die Verfahrensdoku einfrieren

Mitarbeiter: erfassen und bearbeiten; Verfahrensdoku nicht einfrieren

Steuerberater: nur lesen (Schreibzugriffe serverseitig gesperrt)

Anmeldung mit E-Mail und Passwort (gespeichert nur als bcrypt-Hash), Sitzung per geschütztem Cookie.

Eine Zwei-Faktor-Anmeldung für Kunden-Logins gibt es derzeit nicht.

9. Datenzugriff der Finanzverwaltung

1. Z1 (unmittelbar): Nur-Lese-Zugang über eine eigene Anmeldung mit Lese-Rolle oder über die Prüfungsansicht.
2. Z2 (mittelbar): Auswertungen in der App nach Vorgabe des Prüfers.
3. Z3 (Datenüberlassung): Prüfungs-Export als ZIP mit CSV- und JSON-Dateien, Prüfsummen und der Verfahrensdokumentation. Kein zertifiziertes GDPdU-/IDEA-Format.

10. Was Neretha nicht übernimmt

1. Die organisatorischen Teile der Verfahrensdokumentation (wer was wann macht) beschreibt der Kunde selbst; Neretha liefert dafür eine Vorlage.
2. Vollständigkeit der Belege, rechtzeitige Erfassung und die Entscheidung über das Vernichten von Papier liegen beim Kunden.
3. Keine Steuerberatung, keine Garantie für das Ergebnis einer Außenprüfung.

Änderungen dieser Beschreibung

2026.10-1 (28.10.2026): Erste veröffentlichte Fassung.
2026.10-2 (29.10.2026): Betriebsarten getrennt: Diese Beschreibung gilt für den Server-Betrieb (Web-App). Lokaler Betrieb auf eigenem Rechner als eigene Betriebsart mit Sicherung und Aufbewahrung beim Unternehmen ergänzt. Geplante Apps: Mac, Windows, Linux, iOS und Android.