PraxisEasy

PraxisEasy für Windows
Installationshandbuch für die IT

Installation, Softwareverteilung, Zertifikate, Datensicherung, Updates und die technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO.

1 Überblick und Voraussetzungen
2 Installation mit Assistent
3 Stille Installation und Softwareverteilung
4 Ersteinrichtung und Lizenz
5 Arbeitsplätze und Zertifikat
6 Datensicherung, Zweitkopie, Wiederherstellung
7 Updates und Deinstallation
8 Dienste, Ports, Pfade, Protokolle
9 Datenschutz und TOM (Art. 32 DSGVO)
10 Fehlerbehebung

Version 1.2 · Stand 12.10.2026 · gilt für PraxisEasy 1.2.0

PraxisEasy, Inhaber Markus Meyer, Rosenstr. 1a, 92353 Postbauer-Heng · info@praxiseasy.de

© 2026 Markus Meyer · PraxisEasy. Alle Rechte vorbehalten.
Weitergabe innerhalb der lizenzierten Einrichtung erlaubt.

1 Überblick und Voraussetzungen

PraxisEasy für Windows ist die selbst betriebene Ausgabe von PraxisEasy. Das Installationspaket (MSI) enthält alles Nötige: Anwendungsserver (Node.js), Datenbank (PostgreSQL 16) und Oberfläche. Es wird nichts nachgeladen, und PraxisEasy baut von sich aus keine Verbindung ins Internet auf.

Der Funktionsumfang entspricht PraxisEasy Cloud, einschließlich Zulassungs-Check, Leistungseinschätzung nach ILEPA, Beurteilungsbogen für die Pflegeschule als PDF, Jahrgangsplanung mit Schulblöcken, Messenger mit Lesebestätigung, App-Zugang für Auszubildende per Häkchen (Benutzername und Passwort, Auszubildende sehen nur Dienstplan und Anträge) und Plan-Import. Nur das Träger-Netzwerk (Einsatzplatzbörse zwischen Trägern) setzt eine gemeinsame Plattform voraus und ist in der Windows-Ausgabe ausgeblendet. Neue Datenbanktabellen legt PraxisEasy beim Start selbst an.

> **Plan-Import in der Windows-Ausgabe:** Dienst-, Urlaubs-, Schul- und Einsatzpläne lassen sich aus **Excel** (.xlsx, .xls, .ods), **CSV** und **Word** (.docx) übernehmen. Der Import aus **PDF** und **Fotos/Scans** benötigt Texterkennungsprogramme, die nicht zum Windows-Paket gehören; PraxisEasy meldet dann „PDF- und Foto-Import ist in der Windows-Version nicht verfügbar. Bitte Excel, CSV oder Word verwenden.“ Tipp: PDF-Pläne in Word oder Excel öffnen und als .docx bzw. .xlsx speichern.

> **Neu in 1.2.0:** Hochgeladene Dokumente werden auf dem Server mit **AES-256-GCM** verschlüsselt abgelegt (Kapitel 9). Das Lernquiz ist entfallen; vorhandene Quiz-Daten älterer Versionen bleiben unverändert in der Datenbank und stören nicht.

Betriebsart	Einsatz
Einzelplatz	Ein Rechner, eine oder wenige Personen. Erreichbar nur auf diesem Rechner unter `http://localhost:8080`. Keine Firewall-Freigabe.
Intranet-Server	Ein Windows-Rechner oder -Server im Netzwerk der Einrichtung; alle Arbeitsplätze, Tablets und Stationen greifen gleichzeitig per Browser zu. HTTPS auf Port 8443, Umleitung von Port 8080. Firewall-Freigabe nur für Domänen- und private Netzwerke.

Voraussetzung	Wert
Betriebssystem	Windows 10 / 11 (64 Bit) oder Windows Server 2016 und neuer
Arbeitsspeicher	mindestens 4 GB, für den Serverbetrieb mit mehr als 30 gleichzeitigen Nutzern 8 GB
Speicherplatz	ca. 400 MB für das Programm, zusätzlich Daten und Sicherungen (typisch unter 2 GB pro Jahr)
Rechte	Installation mit Administratorrechten; der Dienst läuft danach als eingeschränktes Konto „Netzwerkdienst“
Arbeitsplätze	aktueller Browser (Edge, Chrome, Firefox, Safari); keine Installation auf den Arbeitsplätzen nötig
Internet	nicht erforderlich, weder für Installation noch Betrieb noch Lizenzprüfung

2 Installation mit Assistent

1. `PraxisEasy-1.2.0.msi` als Administrator starten. Die Prüfsumme (SHA-256) steht in der beiliegenden Datei `.sha256.txt`.
2. **Lizenzvertrag** lesen und bestätigen. Ohne Bestätigung ist „Weiter“ gesperrt.
3. **Datenschutz**: Hinweise lesen und die drei Pflichtbestätigungen setzen (Verantwortlichkeit der Einrichtung, keine Patientendaten, Zugriffsschutz und Sicherung). Erst dann geht es weiter.
4. **Betriebsart** wählen: Einzelplatz oder Intranet-Server.
5. Zielordner bestätigen (Standard `C:\Program Files\PraxisEasy`) und installieren.

Die Installation richtet Datenbank, Dienste, Zertifikat (Serverbetrieb), Firewall-Regel (Serverbetrieb), die tägliche Sicherung und die Verknüpfungen ein und prüft zum Schluss, ob PraxisEasy antwortet. Schlägt ein Schritt fehl, wird die Installation vollständig zurückgenommen; das Protokoll steht in `C:\ProgramData\PraxisEasy\logs\installation.log`.

3 Stille Installation und Softwareverteilung

Für Intune, SCCM/MECM oder eigene Skripte. Die Zustimmung zu Lizenzvertrag und Datenschutz muss ausdrücklich übergeben werden; ohne sie bricht die Installation mit einer Meldung ab.

```
msiexec /i PraxisEasy-1.2.0.msi /qn LIZENZ_ZUSTIMMUNG=1 DSGVO_ZUSTIMMUNG=1 MODE=server /l*v
"%TEMP%\praxiseasy-install.log"
```

Eigenschaft	Bedeutung
`LIZENZ_ZUSTIMMUNG=1`	Pflicht. Bestätigt den Lizenzvertrag (LIZENZVERTRAG.txt).
`DSGVO_ZUSTIMMUNG=1`	Pflicht. Bestätigt die Datenschutzhinweise (DATENSCHUTZ.txt) einschließlich der drei Verpflichtungen aus Kapitel 2.
`MODE`	`einzelplatz` (Standard) oder `server`
`PORT`	Port der Anwendung. Standard 8080 (Einzelplatz) bzw. 8443 (Server).
`CERTPFX`, `CERTPASS`	Optional: eigenes Zertifikat der Einrichtung (PFX mit privatem Schlüssel). Ohne Angabe wird ein eigenes Zertifikat erzeugt. Das Kennwort wird im Installationsprotokoll nicht ausgegeben.
`BACKUPDIR`	Optional: Zielordner der täglichen Sicherung, z. B. ein zweites Laufwerk. Standard `C:\ProgramData\PraxisEasy\backups`.
`DATADIR`	Optional: Datenordner. Standard `C:\ProgramData\PraxisEasy`.

> **Gruppenrichtlinie (GPO):** Die Softwareinstallation per GPO kann keine Eigenschaften übergeben. Verwenden Sie dort eine Transformationsdatei (.mst, z. B. mit Orca erstellt) mit den obigen Eigenschaften, oder verteilen Sie per Startskript mit der gezeigten Befehlszeile.

4 Ersteinrichtung und Lizenz

Nach der Installation öffnet die Verknüpfung „PraxisEasy“ die Ersteinrichtung: Name der Einrichtung, erstes Administrationskonto (Passwort mindestens 10 Zeichen mit Groß-, Kleinbuchstaben und Ziffer).

- Auf dem Server selbst ist kein Code nötig. Von einem anderen Rechner aus fragt PraxisEasy nach dem **Einrichtungscode** aus `C:\ProgramData\PraxisEasy\Einrichtungscode.txt` (nur für Administratoren lesbar). Der Code verfällt nach der Einrichtung.
- Die **Lizenz** tragen Administratoren unter Verwaltung › Lizenz ein. Der Schlüssel ist digital signiert und wird ohne Internet geprüft. Ohne Lizenz läuft eine Testversion mit vollem Funktionsumfang für 14 Tage ab der Ersteinrichtung. Danach sind Änderungen gesperrt, bis ein Lizenzschlüssel eingetragen ist; Anzeigen, Exportieren, An- und Abmelden sowie Löschungen nach DSGVO bleiben möglich. Mit Lizenz begrenzt sie nur das Anlegen weiterer Auszubildender (Lizenz S: 15, Lizenz L: 40); vorhandene Daten bleiben immer nutzbar und exportierbar.
- Weitere Personen lädt die Administration per Einladungslink ein oder übernimmt Personaldaten (CSV, Excel, DATEV LODAS, HL7, FHIR).

5 Arbeitsplätze und Zertifikat

Im Serverbetrieb erreichen die Arbeitsplätze PraxisEasy unter `https://<servername>:8443`. Die genaue Adresse steht in `C:\Program Files\PraxisEasy\Zugang.txt`.

Ohne eigenes Zertifikat erzeugt die Installation ein Serverzertifikat (RSA 3072, SHA-256, 5 Jahre gültig) für den Rechnernamen, den vollständigen Domänennamen und `localhost`. Damit die Browser der Arbeitsplätze keine Warnung zeigen, verteilen Sie `C:\ProgramData\PraxisEasy\tls\PraxisEasy-Zertifikat.cer` als vertrauenswürdige Stammzertifizierungsstelle:

```
Gruppenrichtlinie: Computerkonfiguration › Richtlinien › Windows-Einstellungen › Sicherheit
seinstellungen ›
Richtlinien für öffentliche Schlüssel › Vertrauenswürdige Stammzertifizierungsstellen › Imp
ortieren
```

Einzelne Geräte (auch Tablets) laden das Zertifikat unter `http://<servername>:8080/praxiseasy-zertifikat.cer`. Alternativ geben Sie bei der Installation ein Zertifikat Ihrer eigenen Zertifizierungsstelle an (`CERTPFX`); dann ist keine Verteilung nötig.

6 Datensicherung und Wiederherstellung

- Täglich um 01:30 Uhr sichert die geplante Aufgabe „PraxisEasy Sicherung“ Datenbank und Dokumente in eine Datei `praxiseasy_JJJJ-MM-TT_HHmm.pe-sicherung`. Die Datei ist mit **AES-256-GCM** verschlüsselt und gegen Veränderung geschützt. Aufbewahrung 30 Tage.
- Der **Sicherungsschlüssel** steht in `C:\ProgramData\PraxisEasy\WICHTIG-Sicherungsschluessel.txt`. Bewahren Sie ihn getrennt vom Server auf (Passwort-Tresor, Ausdruck im Safe). Ohne ihn kann niemand eine Sicherung wiederherstellen, auch nicht der Hersteller.
- Jede Sicherung enthält auch den **Schlüssel der Dokument-Verschlüsselung** (innerhalb der verschlüsselten Datei). Bei der Wiederherstellung, auch auf einem neu installierten Server, übernimmt PraxisEasy ihn automatisch, damit die Dokumente lesbar bleiben. Es genügt also, den Sicherungsschlüssel aufzubewahren.
- Kopieren Sie die Sicherungsdateien zusätzlich an einen zweiten Ort (zweites Laufwerk, NAS, Bandsicherung). Da sie verschlüsselt sind, dürfen sie auch in einem externen Speicher liegen.

Externe Zweitkopie auf einer Hetzner Storage Box (empfohlen)

Für den Fall eines Brands, Diebstahls oder Verschlüsselungstrojaners kopiert PraxisEasy jede Sicherung zusätzlich auf einen externen Speicher. Empfohlen wird eine eigene **Hetzner Storage Box** (Rechenzentrum in Deutschland). Die Dateien sind vor dem Hochladen verschlüsselt; Hetzner kann sie nicht lesen. Den Vertrag zur Auftragsverarbeitung schließt die Einrichtung online in der Hetzner-Konsole ab.

1. Storage Box bestellen, „SSH-Unterstützung“ und „Externe Erreichbarkeit“ aktivieren, am besten einen eigenen Unterbenutzer für PraxisEasy anlegen.
2. Auf dem PraxisEasy-Server als Administrator ausführen:

```
powershell -ExecutionPolicy Bypass -File "C:\Program Files\PraxisEasy\tools\offsite-einrich
ten.ps1" -Server u123456.your-storagebox.de -Benutzer u123456
```

3. Den angezeigten öffentlichen Schlüssel in der Storage Box hinterlegen (Datei `.ssh/authorized_keys`, Anleitung „Storage Box – SSH-Keys“ von Hetzner) und die Verbindung prüfen:

```
powershell -ExecutionPolicy Bypass -File "C:\Program Files\PraxisEasy\tools\offsite.ps1" -D
ataDir "C:\ProgramData\PraxisEasy" -Pruefen
```

Ab dann wird jede tägliche Sicherung per SFTP (Port 23) übertragen; Kopien älter als 30 Tage werden entfernt. Das Ergebnis steht in `logs\sicherung.log`. Abschalten mit `offsite-einrichten.ps1 -Abschalten`. Voraussetzung ist der in Windows enthaltene OpenSSH-Client (Windows 10 ab 1809, Windows Server ab 2019; bei Server 2016 als Feature nachinstallieren).

Wiederherstellen (als Administrator, der aktuelle Stand wird vorher automatisch gesichert):

```
powershell -ExecutionPolicy Bypass -File "C:\Program Files\PraxisEasy\tools\wiederherstelle
n.ps1" -Datei "D:\Sicherung\praxiseasy_2026-10-01_0130.pe-sicherung"
```

Stammt die Sicherung von einem anderen Server, geben Sie dessen Schlüssel mit `-Schluessel <64 Zeichen>` an.

7 Updates und Deinstallation

- **Update:** neue MSI-Datei wie in Kapitel 2 oder 3 installieren. Datenbank, Dokumente, Schlüssel, Zertifikat und Lizenz bleiben erhalten; die Datenbankstruktur wird beim Start automatisch angepasst. Legen Sie vorher eine Sicherung an.
- **Update von 1.1.x auf 1.2.0:** Die Installation erzeugt einmalig den Schlüssel der Dokument-Verschlüsselung (256 Bit, in `config\praxiseasy.env`) und verschlüsselt alle vorhandenen Dokumente; jede Datei wird danach durch Entschlüsseln geprüft. Das Ergebnis steht in `logs\installation.log`. Prüfen lässt sich der Stand jederzeit mit `node app\backend\uploads-verschluesseln.js --pruefen` (mit gesetzten Umgebungsvariablen `UPLOAD_KEY` und `UPLOAD_DIR` aus der Konfiguration).
- **Deinstallation** über „Apps“ bzw. `msiexec /x PraxisEasy-1.2.0.msi`. Dienste, Aufgabe, Firewall-Regel und Verknüpfungen werden entfernt, die **Daten bleiben erhalten**.
- Endgültiges Löschen aller Daten (Datenbank, Dokumente, Sicherungen, Schlüssel, Zertifikat):

```
msiexec /x PraxisEasy-1.2.0.msi DATEN_LOESCHEN=1
```

> Das endgültige Löschen ist nicht rückgängig zu machen. Beachten Sie vorher die Aufbewahrungsfristen für Ausbildungsnachweise und erstellen Sie gegebenenfalls einen Komplettexport (Verwaltung › Einrichtung).

8 Dienste, Ports, Pfade, Protokolle

Bestandteil	Details
Dienst `PraxisEasyDB`	PostgreSQL 16, Konto Netzwerkdienst, nur `127.0.0.1:55432`, Anmeldung scram-sha-256
Dienst `PraxisEasyApp`	Anwendungsserver, Konto Netzwerkdienst, abhängig von PraxisEasyDB, Neustart bei Fehlern
Ports	Einzelplatz: 8080 nur lokal. Server: 8443 (HTTPS), 8080 (Umleitung und Zertifikat-Download)
Firewall	Regel „PraxisEasy (Intranet)“, nur Profile Domäne und Privat, nur im Serverbetrieb
Programm	`C:\Program Files\PraxisEasy` (Zugang.txt, LIZENZVERTRAG.txt, DATENSCHUTZ.txt, DRITTANBIETER-LIZENZEN.txt)
Daten	`C:\ProgramData\PraxisEasy`: db, uploads, backups, config, tls, logs. Zugriff nur SYSTEM, Administratoren, Netzwerkdienst
Protokolle	`logs\installation.log`, `logs\sicherung.log`, `logs\PraxisEasyApp*.log`, `logs\datenbank\` (7 Tage rollierend)
Geplante Aufgabe	`\PraxisEasy\PraxisEasy Sicherung`, täglich 01:30, als SYSTEM

9 Datenschutz und technische und organisatorische Maßnahmen (TOM)

Die Einrichtung ist Verantwortliche (Art. 4 Nr. 7 DSGVO). Der Hersteller hat keinen Zugriff auf die Daten; ein Vertrag zur Auftragsverarbeitung ist daher nur bei beauftragter Fernwartung nötig. Die folgende Übersicht kann in das Verzeichnis von Verarbeitungstätigkeiten und die eigene TOM-Dokumentation übernommen werden.

Schutzziel	Maßnahme in PraxisEasy
Vertraulichkeit: Zugang	Anmeldung mit persönlichem Konto; Passwörter nur als bcrypt-Prüfwert; Sperre nach 8 Fehlversuchen; optionale Zwei-Faktor-Anmeldung (TOTP), für alle Konten erzwingbar; Sitzungen serverseitig widerrufbar; automatische Abmeldung bei Inaktivität
Vertraulichkeit: Zugriff	Rollen (Administration, Pflegedienstleitung, Praxisanleitung, Auszubildende, Pflegeschule, externe Einsatzstelle) mit abgestuften Rechten; Auszubildende sehen nur eigene Daten; Trennung von Einrichtungen in der Datenbank mit automatischer Prüfung
Vertraulichkeit: Übertragung	HTTPS (TLS 1.2+) im Netzwerk, HSTS; Datenbank nur lokal erreichbar; keine Übermittlung an den Hersteller oder Dritte, keine Telemetrie, keine externen Inhalte (Schriften und Programmteile lokal), Sicherheitsrichtlinie (CSP) im Browser
Vertraulichkeit: Speicherung	Datenordner nur für SYSTEM, Administratoren und den Dienst; hochgeladene Dokumente einzeln mit AES-256-GCM verschlüsselt (256-Bit-Schlüssel je Installation, zufälliger IV je Datei, Manipulationsschutz per Authentifizierungs-Tag); Sicherungen AES-256-GCM verschlüsselt; Empfehlung: BitLocker auf dem Server (schützt zusätzlich die Datenbank)
Integrität	Änderungsprotokoll wichtiger Vorgänge (30 Tage, ohne IP-Adressen); Konfliktschutz bei gleichzeitiger Bearbeitung; signierte Lizenz; manipulationssichere Sicherungsdateien (Authentifizierung per GCM)
Verfügbarkeit	Dienste mit automatischem Neustart; tägliche Sicherung mit 30 Tagen Aufbewahrung; optionale verschlüsselte Zweitkopie extern (Hetzner Storage Box, Deutschland); dokumentierte Wiederherstellung; Weiterarbeit bei kurzen Verbindungsunterbrechungen mit späterer Übertragung
Datensparsamkeit, Löschung	Keine Patientendaten (Warnhinweis im Messenger); Aufbewahrungsfristen einstellbar; Deaktivierung und Löschung ausgeschiedener Personen; Konto-Selbstlöschung; Komplettexport und Datenauskunft (Art. 15, 20 DSGVO) per Knopfdruck
Organisatorisch (Einrichtung)	Server-Updates und Virenschutz; Zugriffsschutz auf den Server; Sicherungsschlüssel getrennt verwahren; Sicherungen an zweitem Ort; Beschäftigte informieren (Art. 13 DSGVO); Datenschutzbeauftragte und ggf. Mitarbeitervertretung einbeziehen

10 Fehlerbehebung

Problem	Lösung
Installation bricht mit Hinweis auf Zustimmung ab	`LIZENZ_ZUSTIMMUNG=1 DSGVO_ZUSTIMMUNG=1` angeben (Kapitel 3)
„PraxisEasy antwortet nicht“	`logs\installation.log` und `logs\PraxisEasyApp.err.log` prüfen; Port belegt? Anderen Port mit `PORT=` wählen
Browser warnt vor dem Zertifikat	Zertifikat verteilen (Kapitel 5) oder eigenes Zertifikat verwenden
Arbeitsplatz erreicht den Server nicht	Netzwerkprofil des Servers muss „Domäne“ oder „Privat“ sein; Firewall-Regel „PraxisEasy (Intranet)“ prüfen
Ersteinrichtung verlangt einen Code	Code aus `Einrichtungscode.txt` im Datenordner verwenden oder die Einrichtung direkt am Server vornehmen
Zweitkopie fehlgeschlagen	`logs\sicherung.log` prüfen; Verbindung mit `offsite.ps1 -Pruefen` testen; Schlüssel in der Storage Box hinterlegt? SSH-Unterstützung aktiv?
Plan-Import meldet „in der Windows-Version nicht verfügbar“	PDF und Fotos werden unter Windows nicht gelesen; Plan als Excel, CSV oder Word (.docx) speichern und erneut importieren
Dokument lässt sich nicht öffnen („Datei konnte nicht gelesen werden“)	Schlüssel der Dokument-Verschlüsselung passt nicht zur Datei, z. B. nach manuellem Kopieren des Upload-Ordners. Daten über `wiederherstellen.ps1` zurückspielen, das übernimmt den passenden Schlüssel
Sicherung fehlgeschlagen	`logs\sicherung.log` prüfen; Speicherplatz und Rechte des Zielordners (SYSTEM benötigt Schreibrecht)