FOCUS FAMILY

ISO-Konformitätsprofil

Was Focus Family für Ihre Zertifizierung leistet – und was nicht

Software Notion · Kornblumenring 40 · 31600 Uchte · Produktstand 1.3.0 · Prüfstand 01.11.2026

Inhaltsverzeichnis

1. **Über dieses Dokument**
   1. Wozu es da ist
   2. Was es ausdrücklich nicht ist
   3. Prüfgrundlage
2. **Das Wichtigste in Kürze**
   1. Gesamtbild
   2. Sechs Kernaussagen
3. **Wie Normen und Software zusammenhängen**
   1. Zertifiziert wird die Organisation, nicht die Software
   2. Was das für Ihre Prüfung bedeutet
4. **Verantwortungsteilung Hersteller ↔ Träger**
5. **ISO/IEC 27001 – Informationssicherheits-Managementsystem**
   1. Was die Software liefert
   2. Was Sie selbst leisten müssen
   3. Wo es aktuell hakt
6. **ISO/IEC 27034 – Anwendungssicherheit**
   1. Worum es in dieser Norm geht
   2. Was die Software liefert
   3. Was Sie selbst leisten müssen
   4. Wo es aktuell hakt
7. **ISO/IEC 25010 – Software-Produktqualität**
   1. Funktionale Eignung – erfüllt
   2. Leistungseffizienz – teilweise
   3. Kompatibilität – erfüllt
   4. Interaktionsfähigkeit – teilweise
   5. Zuverlässigkeit – erfüllt
   6. Sicherheit – erfüllt
   7. Wartbarkeit – erfüllt
   8. Flexibilität – erfüllt
   9. Sicherheit im Sinne von Gefahrlosigkeit – teilweise
8. **ISO/IEC 29147 und 30111 – Umgang mit Schwachstellen**
   1. Worum es geht
   2. Stand
   3. Was faktisch schon funktioniert
   4. Was das für Sie heute bedeutet
9. **Wo Focus Family Ihre Zertifizierung aktuell erschwert**
10. **Bewusste Grenzen des Produkts**
11. **Datenschutz und Offenheit**
    1. Keine Herstellerbindung Ihrer Daten
    2. Datenschutz als Funktionsbestandteil
    3. Wo Offenheit heute endet
12. **Offene Punkte und geplante Verbesserungen**
13. **Nachweisverzeichnis**
14. **Fragen, die Sie uns stellen sollten**
15. **Kontakt und Gültigkeit**

Über dieses Dokument

Wozu es da ist

Sie prüfen gerade, ob Focus Family in Ihrer Einrichtung eingesetzt werden kann. Wenn Ihr Träger ein Informationssicherheits-Managementsystem betreibt, bereits nach ISO/IEC 27001 zertifiziert ist oder eine Zertifizierung anstrebt, müssen Sie für jedes eingesetzte Fachverfahren beantworten können: **Welche Sicherheitsmaßnahmen übernimmt die Software, welche müssen wir selbst erbringen, und wo bleiben Lücken?**

Dieses Dokument beantwortet genau diese drei Fragen – für vier Normen:

Norm	Thema
ISO/IEC 27001:2022	Informationssicherheits-Managementsystem (ISMS)
ISO/IEC 27034	Anwendungssicherheit (Application Security)
ISO/IEC 25010:2023	Software-Produktqualität
ISO/IEC 29147 / 30111	Umgang mit Schwachstellen (Meldung und Behandlung)

Was es ausdrücklich nicht ist

Dieses Dokument ist **kein Zertifikat**, **kein Prüfbericht einer akkreditierten Stelle** und **keine Zusicherung von Normkonformität**. Es ist eine Selbstauskunft des Herstellers, erstellt durch eine strukturierte Prüfung des tatsächlichen Quellcodes, der Konfiguration und der Dokumentation. Sie dürfen jede Aussage hierin hinterfragen – Abschnitt „Nachweisverzeichnis" nennt zu jeder Aussage das Artefakt, mit dem sie belegt ist.

Wir halten uns an eine einfache Regel: **lieber eine unbequeme Lücke benennen als eine Zusicherung, die im Ernstfall nicht hält.** Sie finden deshalb in diesem Dokument einen ausführlichen Abschnitt darüber, was Focus Family **nicht** kann und wo es Ihre Zertifizierung aktuell **erschwert**.

Prüfgrundlage

Angabe	Wert
Produktstand	1.3.0
Prüfdatum	1. November 2026 (Version 1.3.0, Build 26302)
Prüfmethode	Quellcode-Durchsicht, Konfigurations- und Deployment-Review, Dokumentenabgleich, Testlauf
Prüftiefe	Alle sicherheitsrelevanten Codepfade des Servers, der Synchronisation und der Verschlüsselung
Testnachweis	6.061 Tests: 6.047 bestanden, 14 übersprungen (umgebungsabhängig), 0 fehlgeschlagen; ein vollständiger Lauf aller sieben Testreihen am Prüfdatum, Server- und Lizenzserverreihe gegen zwei PostgreSQL-17-Instanzen einschließlich Aktualisierungstest ab Version 1.0.0, ohne übersprungene Datenbanktests
Nicht geprüft	Laufzeitverhalten Ihrer konkreten Installation, Ihre Betriebsumgebung, Ihre organisatorischen Abläufe

---

Das Wichtigste in Kürze

Gesamtbild

Norm	Reifegrad	Kurzbewertung
ISO/IEC 27001	**unterstützend, gut**	Die technischen Maßnahmen aus Anhang A sind weitgehend umgesetzt und belegbar; von 66 adressierbaren Maßnahmen 40 vollständig und 26 teilweise, keine offen. Die Software liefert Ihnen außerdem automatisch erzeugte Nachweisdokumente.
ISO/IEC 27034	**teilweise**	Alle inhaltlichen Bestandteile sind vorhanden (Anforderungsspezifikation, Bedrohungsmodell, Maßnahmen, Prüfungen); Maßnahmenbibliothek und Vertrauensniveau sind noch nicht in der von der Norm erwarteten Form gebündelt. Hier liegt das größte kurzfristige Potenzial.
ISO/IEC 25010	**gut, drei Merkmale teilweise**	Sechs von neun Qualitätsmerkmalen sind vollständig belegt; Leistungseffizienz, Interaktionsfähigkeit und Gefahrlosigkeit teilweise. Die für Sie wichtigste offene Stelle ist die **Barrierefreiheit**: Beschriftungen für Bildschirmlesegeräte sind vollständig und eine Erklärung liegt vor, eine Prüfung mit echten Hilfsmitteln steht aus.
ISO/IEC 29147 / 30111	**eingerichtet, noch nicht erprobt**	Meldeweg veröffentlicht und Postfach eingerichtet (`security.txt` , Fristen nach Schweregrad), Behebungsprozess mit Rollen und Fristen beschrieben, Meldefunktion in Admin-Panel, App und Desktop. Da bisher keine Auslieferung eine gemeldete Schwachstelle schließen musste, sind Offenlegung, Sicherheitsmeldung und Nachbetrachtung beschrieben, aber noch nie durchlaufen.

Sechs Kernaussagen

1. **Ihre Daten bleiben bei Ihnen.** Es gibt keine Hersteller-Cloud. Der Server läuft in Ihrer Infrastruktur, unter Ihrer Kontrolle, mit Ihren Schlüsseln. Der Hersteller hat keinen Zugang zu Ihren Falldaten – weder technisch noch vertraglich vorgesehen. Daten verlassen Ihre Installation an Fremdsysteme nur über Schnittstellen, die Sie selbst einrichten und die Ihre Datenschutzrolle im Vier-Augen-Prinzip freigibt.
2. **Auf den Endgeräten sind alle Fachdaten verschlüsselt.** AES-256-GCM, Schlüssel im Betriebssystem-Schlüsselspeicher. Ein verlorenes Gerät gibt ohne Gerätesperre und App-Sperre nichts preis.

3. **Es gibt keine Ende-zu-Ende-Verschlüsselung.** Wer administrativen Zugriff auf Ihren Server, Ihre Datenbank, Ihr Dateisystem oder Ihr Schlüsselmaterial hat, kann synchronisierte Inhalte technisch lesen. Das ist eine bewusste Entscheidung der Version 1 und wird nirgends anders dargestellt.
4. **Die Software erzeugt Ihre Datenschutz-Nachweise selbst.** Verzeichnis technischer und organisatorischer Maßnahmen (Art. 32 DSGVO), AVV-Vorlage, Löschkonzept und Auskunftsschreiben entstehen aus der **echten Konfiguration Ihrer Instanz** – nicht aus einer Textvorlage. Die Dokumentation kann dadurch nicht von der Realität abweichen.
5. **Das Audit-Protokoll ist gegen die Anwendung selbst geschützt, Schlüssel sind rotierbar.** Die Anwendung kann ihre eigenen Protokolleinträge weder ändern noch löschen, und jeder Eintrag ist mit seinem Vorgänger verkettet — Änderung, Entfernung und Abschneiden fallen bei der Prüfung auf. Gegen jemanden mit vollem Datenbankzugriff, der einen älteren Gesamtstand zurückspielt, schützt das nicht; dafür exportieren Sie das Protokoll. Verschlüsselungsschlüssel für Gerätedaten, Anhänge und Serverdateien lassen sich im laufenden Betrieb austauschen.
6. **Zwei Dinge fehlen, die Sie kennen müssen:** mitgelieferte Alarmregeln für die Überwachung, und eine mit Hilfsmitteln geprüfte Barrierefreiheit. Beide sind in Abschnitt „Offene Punkte" mit Status benannt.

Wie Normen und Software zusammenhängen

Dieser Abschnitt klingt akademisch, entscheidet aber darüber, ob Ihre Prüfung sauber wird.

Zertifiziert wird die Organisation, nicht die Software

ISO/IEC 27001 zertifiziert ein **Managementsystem einer Organisation** – Ihre Organisation. Es gibt keine ISO-27001-Zertifizierung für ein Softwareprodukt, und jeder Anbieter, der Ihnen eine solche anbietet, sagt etwas Unzutreffendes.

Was eine Software leisten kann, ist dreierlei:

1. Die **technischen Maßnahmen** aus Anhang A umsetzen, die Ihr ISMS ohnehin fordert (Zugriffssteuerung, Verschlüsselung, Protokollierung, Schutz vor Schadsoftware …).
2. Ihnen die **Nachweise** liefern, mit denen Sie gegenüber dem Auditor belegen, dass diese Maßnahmen wirken.
3. Ihrer Zertifizierung **nicht im Weg stehen** – also keine Eigenschaft mitbringen, die eine Anforderung Ihres ISMS unmöglich macht.

Focus Family erfüllt Punkt 1 und 2 weitgehend. Zu Punkt 3 finden Sie in Abschnitt „Wo Focus Family Ihre Zertifizierung aktuell erschwert" eine vollständige, ungeschönte Liste.

Was das für Ihre Prüfung bedeutet

Sie können dieses Dokument als **Lieferantenauskunft** in Ihre Maßnahme A.5.19–A.5.22 (Lieferantenbeziehungen) einhängen. Es ersetzt weder Ihre eigene Risikobewertung noch den Auftragsverarbeitungsvertrag – aber es liefert Ihnen die Faktenbasis für beides.

Verantwortungsteilung Hersteller ↔ Träger

Die häufigste Ursache für Lücken in Audits ist eine Maßnahme, von der beide Seiten annahmen, die jeweils andere kümmere sich darum. Diese Tabelle beugt dem vor.

Maßnahmenbereich	Hersteller (Software Notion)	Träger (Sie)
Verschlüsselung auf Endgeräten	Umsetzung, Schlüsselerzeugung, Speicherung im OS-Schlüsselspeicher	Gerätesperre erzwingen, App-Sperre per Richtlinie aktivieren
Verschlüsselung auf dem Server	Dateianhänge verschlüsselt im Ruhezustand	**Datenbank- und Volume-Verschlüsselung**, Schlüsselverwahrung
Schlüsselverwahrung	Erzeugungsverfahren, Dokumentation	**Sicherung, getrennte Aufbewahrung, Zugriffsschutz**
Zugriffssteuerung	Rollen-/Rechtemodell, serverseitige Durchsetzung, Rechte-Obergrenze bei Kontoänderungen, sofortiger Entzug beim Deaktivieren	Rechtevergabe, **regelmäßige Rezertifizierung der Rechte**
Zwei-Faktor-Authentifizierung	TOTP und Passkeys implementiert; Anmeldung über den eigenen Identitätsanbieter (OpenID Connect, SAML 2.0)	**Aktivierung per Richtlinie** (Voreinstellung: aus) bzw. MFA-Pflicht im Identitätsanbieter
Protokollierung	Audit-Protokoll mit über 130 Ereignisarten, Abrufschnittstelle, Weiterleitung der Audit-Kette an ein SIEM (Syslog über TLS oder CEF)	**Auswertung, Aufbewahrung, Alarmierung, Betrieb des SIEM**
Datensicherung	Skripte, geprüftes Wiederherstellungsverfahren	**Durchführung, Aufbewahrung, Verschlüsselung, Wiederherstellungstests**
Schadsoftwareschutz	ClamAV-Anbindung, in Produktion fail-closed	**Betrieb und Signaturaktualisierung des Scanners**
Schwachstellenbehandlung	Behebung, Bereitstellung neuer Versionen als signiertes Update mit Schutz vor Rückstufung	**Einspielen der Updates**
Schwachstellenmeldung	Meldeweg, Fristen und Meldefunktion im Produkt	Meldungen absetzen; Fristen in die Lieferantenakte aufnehmen
Löschfristen	Konfigurierbar; Änderungsprotokoll, Löschmarkierungen und Auskunftsdaten werden automatisch bereinigt	**Fristen festlegen; Aufbewahrung von Audit- und Anwendungsprotokollen regeln**
Physische Sicherheit	—	**vollständig bei Ihnen**
Personelle Maßnahmen	—	**vollständig bei Ihnen** (Schulung, Verpflichtung, Ausscheiden)
Schnittstellen zu Fremdsystemen	Standardschnittstellen, Freigabe durch die Datenschutzrolle im Vier-Augen-Prinzip, Datenschutz-Voreinstellungen, Offenlegungsverzeichnis, Transportabsicherung, Not-Aus, Vorlagen für DSFA und Verarbeitungsverzeichnis	**Zweck und Rechtsgrundlage je Schnittstelle, Freigabe, Absicherung und Löschung in den Zielsystemen, Vereinbarungen mit deren Betreibern**
Netzzugang	Beschränkung des Admin-Panels auf Intranet/VPN, festes Proxy-Netz, optionale Hostbindung	**Netzsegmentierung, Reverse Proxy, Freigabe der ausgehenden Verbindungen**
Notfallvorsorge	Offline-Fähigkeit der Apps, Wiederherstellungsverfahren	**Wiederanlaufziele, Notfallübungen, Ersatzverfahren**
Barrierefreiheit	Beschriftungen für Bildschirmlesegeräte, Erklärung zur Barrierefreiheit	Verbleibende Einschränkungen in Ihre eigene Erklärung übernehmen

ISO/IEC 27001 – Informationssicherheits-Managementsystem

Was die Software liefert

Von den 93 Maßnahmen des Anhangs A sind 66 überhaupt durch eine Software adressierbar; die übrigen 27 betreffen Ihre Organisation, Ihre Personalprozesse und Ihre Räumlichkeiten oder sind nicht anwendbar. Von diesen 66 sind **40 vollständig und 26 teilweise umgesetzt, keine offen**. Teilweise heißt: Die Maßnahme ist technisch vorhanden, aber ein Teil hängt von Ihrer Konfiguration oder Ihrem Betrieb ab — die Einzelheiten stehen im Anhang.

Besonders belastbar sind:

Zugriffssteuerung (A.5.15, A.8.2, A.8.3). Jede Lese- und Schreiboperation wird auf dem Server gegen den aktuellen Datenbankzustand autorisiert – niemals gegen Angaben des Clients. Die Sichtbarkeitsfilterung geschieht bereits in der Datenbankabfrage, nicht nachträglich im Code. Ein unberechtigter Direktzugriff auf einen bekannten Datensatz liefert „nicht gefunden" statt „verboten", verrät also nicht einmal die Existenz.

Rollentrennung (A.5.3). 64 einzeln vergebbare Berechtigungen, gegliedert in Technik, Fachlichkeit und Datenschutz sowie zwei allgemeine Lizenzrechte. Administrative Rechte erweitern den Zugriff auf Fallinhalte **nicht**. Konten der technischen Administration und des Datenschutzes können sich in den Apps überhaupt nicht anmelden. Betroffenenauskünfte werden nur im Vier-Augen-Prinzip freigegeben. Eine **Rechte-Obergrenze** gilt für jede Kontoänderung: Niemand bearbeitet, deaktiviert oder setzt Anmeldedaten eines Kontos zurück, das Rechte außerhalb des eigenen Vergaberahmens besitzt; auf Bereiche beschränkte Administratorinnen und Administratoren ändern nur Konten, die vollständig in ihrem Bereich liegen, und vergeben keine Verwaltungsrechte für die gesamte Organisation. Schnittstellen richtet die technische Administration ein; Datenflüsse mit Falldaten gibt nur eine andere Person mit Datenschutzrecht frei, die die Schnittstelle weder angelegt noch zuletzt geändert hat. Eingänge aus Schnittstellen prüft und übernimmt nur, wer dafür das eigene Recht besitzt.

Anmeldung und Entzug (A.5.16, A.5.17, A.5.18, A.8.5). Neben Passwort mit TOTP und Passkeys kann die Anmeldung an den eigenen Identitätsanbieter abgegeben werden (OpenID Connect oder SAML 2.0, etwa Microsoft Entra ID oder AD FS); der Server stellt danach weiterhin eigene Token aus. Konten werden nur über vom Anbieter bestätigte Identitäten verknüpft. Ist „SSO erzwingen" aktiv, werden lokale Sitzungen und Token beim Einschalten widerrufen; nur lokale Systemadministrationskonten behalten als Notfallzugang einen Passwortzugang, und zwar ausschließlich zum Admin-Panel. Die Pflicht zur starken Anmeldung gilt für Panel und Synchronisation nach derselben Regel. Ein deaktiviertes Konto verliert seinen Zugang sofort: Sitzungen und Token werden widerrufen, die Synchronisation weist veraltete Anmeldestände ab. Die Anmeldung antwortet für unbekannte, gesperrte und falsche Zugangsdaten einheitlich und mit gleichem Rechenaufwand; Konto-, MFA- und Notfallzugriffs-Endpunkte sind mengenbegrenzt und sperren nach Fehlversuchen. Fachkräfte-Konten lassen sich über SCIM

2.0 aus dem eigenen Identitätsmanagement anlegen und deaktivieren; Rechte sind über SCIM nicht änderbar, Konten mit Verwaltungsrechten sind für SCIM unsichtbar, und das Deaktivieren widerruft die Anmeldesitzungen.

Kryptografie (A.8.24). AES-256-GCM für Fachdaten auf den Geräten und für Dateianhänge auf dem Server, PBKDF2-HMAC-SHA256 mit 310.000 Iterationen für App-Backups, ECDSA P-256 für Gerätenachweise und Lizenzsignaturen. Zugangsdaten, Geheimnisse und Client-Zertifikate der Schnittstellen liegen mit Data Protection verschlüsselt vor und werden nie exportiert; Sendungen über FIT-Connect werden für den Zustellpunkt verschlüsselt, dessen Schlüssel gegen die Verwaltungs-PKI geprüft wird. Kein Einsatz veralteter Verfahren für Sicherheitszwecke.

Gerätebindung (A.8.5). Jedes Endgerät besitzt ein eigenes Schlüsselpaar im Betriebssystem-Schlüsselspeicher. Jede Anfrage trägt einen signierten Gerätenachweis; verbrauchte Nachweise werden gespeichert, sodass ein mitgeschnittener Nachweis nicht wiederverwendet werden kann. Anfragen ohne Gerätekennung werden abgewiesen. **Gestohlene Zugangsdaten allein genügen nicht für einen API-Zugriff.** Einrichtungslinks und -QR-Codes übernimmt eine App erst nach zweistufiger Bestätigung und nur im entsperrten Zustand.

Endgeräte (A.8.1). Die App-Sperre erscheint unter iOS in einem eigenen Fenster über allen Systemdialogen. Gelingt ihre Darstellung nicht, deckt eine undurchsichtige Ersatzfläche die App ab, und solange die App gesperrt ist, ist keine Navigation möglich. Unter iOS und Android sind die App-Daten von Cloud- und Computer-Backups sowie von der Geräteübertragung ausgenommen; fehlt nach einem Gerätewechsel der Schlüssel, zeigt die App eine Wiederherstellungsseite und erzeugt nie einen neuen Schlüssel über vorhandene Daten. Das Navigationsprotokoll für Diagnoseberichte enthält keine Fallkennungen und keine Parameterwerte.

Konfiguration und Netz (A.8.9, A.8.20, A.8.22). Das Admin-Panel lässt sich auf Intranet oder VPN beschränken; der Reverse Proxy liegt in einem festen Netz, nur ihm werden weitergeleitete Absenderangaben geglaubt, zulässige Hostnamen lassen sich festlegen. Alle Verwaltungsaktionen sind gegen Anfragefälschung geschützt (ein Regressionstest prüft jede Aktion), auch Fehlerseiten tragen die Sicherheitskopfzeilen, und der Lizenzdienst wird außerhalb der Entwicklung nur über HTTPS angesprochen. Das eingebaute Aktualisierungsverfahren verweigert Rückstufungen und Versionsabweichungen innerhalb des signierten Pakets.

Informationsübertragung über Schnittstellen (A.5.14, A.8.21, A.8.26). Für die Anbindung von Fachverfahren, DMS und E-Akte, Jugendämtern, Identitätsmanagement, Kalendern und SIEM stehen Standardschnittstellen bereit: REST/JSON mit OAuth 2.0 Client Credentials (`private_key_jwt`), Webhooks mit Signatur nach Standard Webhooks, CMIS 1.1 als Client und Repository, XÖV/xdomea über Verzeichnis, SFTP, XTA 2 und FIT-Connect, SCIM 2.0, iCalendar-Abos und Syslog über TLS bzw. CEF. Jede Schnittstelle trägt Zweck und Rechtsgrundlage und entsteht als Entwurf; Datenflüsse mit Falldaten werden erst nach der Freigabe aktiv, und die Freigabe ist an den geprüften Stand gebunden. Die Voreinstellungen sind datensparsam: pseudonymisiert, nur finale Dokumente, Notizen und vertrauliche Dokumenttypen gesperrt, eingehende Richtung aus. Jede erfolgreiche Übermittlung mit Fallbezug wird im Offenlegungsverzeichnis festgehalten und erscheint im Auskunftspaket nach Art. 15 DSGVO. Ausgehende Verbindungen gehen nur über HTTPS, folgen keinen Weiterleitungen, prüfen die Zieladresse beim Verbindungsaufbau gegen SSRF und lassen sich mit eigener CA, SPKI-Pin und mTLS binden; SFTP verlangt einen bestätigten Hostschlüssel. Eingehende Zugriffe verlangen eine IP-Allowlist (leer heißt gesperrt), sind mengenbegrenzt und an Bereiche gebunden; eingelieferte Dateien durchlaufen Typprüfung und Virenscan, XML wird ohne DTD gelesen, Pakete nur mit Größengrenzen entpackt. Eingänge landen in einem Posteingang mit eigenem Recht. Die endgültige Löschung eines Falls erfasst auch die Kopien in den Schnittstellen. Ein Not-Aus stoppt alle ausgehenden Übertragungen, wiederholt scheiternde Verbindungen pausieren automatisch, und ohne gültige Organisationslizenz ruhen Zustellungen und Zugriffe der Schnittstellen; nur die Weiterleitung der Audit-Kette an das SIEM läuft weiter.

Datensparsamkeit auf den Geräten (A.8.11, A.8.12). Pseudonymisierte Aktenvorblätter nennen statt Namen, Anschrift und Geburtsdatum nur Platzhalter, Wohnort und Geburtsjahr und enthalten weder Telefonnummern, E-Mail-Adressen, Geburtsort, Krankenversicherung noch Kindergeldnummer; Leitweg-IDs für E-Rechnungen werden verschlüsselt gespeichert; unverschlüsselte Zwischen- und Exportdateien liegen nur in Ordnern, die die App regelmäßig bereinigt. Offene Synchronisationskonflikte liegen wie der übrige Bestand verschlüsselt vor, und Kontaktkarten und Einrichtungen führen keine Namen im unverschlüsselten Suchindex der lokalen Datenbank.

Schutz vor Schadsoftware (A.8.7). Hochgeladene Dateien durchlaufen Typ-Allowlist, Magic-Byte-Prüfung, Größenbegrenzung und einen Virenscanner. Erst nach dem Befund „sauber" wird eine Datei ausgeliefert. Ist der Scanner in Produktion nicht erreichbar, werden Uploads **abgelehnt** statt ungeprüft durchgelassen.

Änderungsmanagement (A.8.32). Schemaänderungen laufen ausschließlich über einen transaktionalen Migrator mit Änderungsregister und Datenbanksperre. Ein fehlgeschlagener Schritt rollt vollständig zurück. Es gibt keinen Pfad für unkontrollierte Schemaänderungen im Betrieb.

Automatisch erzeugte Nachweisdokumente (A.5.31, A.5.34). Dies ist die für Ihr Audit wertvollste Eigenschaft: Das Verzeichnis technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO, die AVV-Vorlage, das Löschkonzept und Auskunftsschreiben werden aus der **Live-Konfiguration Ihrer Instanz** erzeugt – inklusive tatsächlich aktiver Zwei-Faktor-Pflicht, konfigurierter Dateitypen, Sitzungsdauer und Kontenzahlen. Eine Abweichung zwischen Dokumentation und Realität ist damit ausgeschlossen.

Was Sie selbst leisten müssen

Die Software kann Ihnen 27 der 93 Maßnahmen nicht abnehmen. Die wichtigsten:

- **Informationssicherheitsleitlinie, Risikobewertung, Anwendbarkeitserklärung (SoA), interne Audits, Managementbewertung** – das Kernstück Ihres ISMS.
- **Alle acht personenbezogenen Maßnahmen** (A.6): Überprüfung von Beschäftigten, Schulung, Verpflichtung auf Vertraulichkeit, Regelungen beim Ausscheiden.
- **Alle vierzehn physischen Maßnahmen** (A.7): Serverraum, Zutritt, Verwahrung mobiler Geräte, sichere Entsorgung.
- **Auswertung der Protokolle und Alarmierung.** Die Software erzeugt die Daten und stellt eine Abrufschnittstelle bereit; die Überwachung ist Ihre Aufgabe.
- **Datensicherung und Wiederherstellungstests.** Verfahren und Skripte sind dokumentiert und einmal nachweislich durchlaufen; die regelmäßige Durchführung liegt bei Ihnen.
- **Rezertifizierung der Zugriffsrechte.** Die Vergabe ist protokolliert, eine turnusmäßige Überprüfung müssen Sie organisatorisch aufsetzen.
- **Bewertung und Freigabe jeder Schnittstelle (A.5.14, A.5.19–A.5.22).** Zweck, Rechtsgrundlage, Datenschutz-Folgenabschätzung und Verarbeitungsverzeichnis (Vorlagen liegen bei), Vereinbarungen mit den Betreibern der Zielsysteme und die Löschung der dorthin übermittelten Daten liegen bei Ihnen.
- **Zeitsynchronisation des Servers (A.8.17).** Die Anforderung und ihre Prüfung (`timedatectl status` , `chronyc tracking`) stehen im technischen Handbuch; der Betrieb eines NTP-Dienstes auf dem Wirt und dessen Überwachung liegen beim Betreiber.

Wo es aktuell hakt

Punkt	Auswirkung auf Ihr Audit
Zwei-Faktor-Authentifizierung ist standardmäßig aus	Eine frisch installierte Instanz erlaubt Anmeldung ohne zweiten Faktor. Sie müssen die Richtlinie aktiv setzen. Wir empfehlen, das zum Pflichtschritt Ihrer Inbetriebnahme zu machen.
XTA 2 und FIT-Connect nur gegen Spezifikations-Mocks geprüft	Die beiden Transporte für die Aktenabgabe sind spezifikationskonform umgesetzt und gegen eigene Nachbildungen getestet; eine Abnahme gegen eine echte Gegenstelle steht aus (Befund F-33). Betrifft A.8.29. Führen Sie vor der produktiven Nutzung eine Testübertragung mit Ihrer Gegenstelle durch.

ISO/IEC 27034 – Anwendungssicherheit

Worum es in dieser Norm geht

ISO/IEC 27034 beschreibt, wie ein Hersteller Anwendungssicherheit **systematisch und nachweisbar** betreibt. Kern ist die Idee, dass jede Sicherheitsmaßnahme (*Application Security Control*) mit einer **zugehörigen Prüfung** verbunden ist, mit der sich ihre Wirksamkeit messen lässt. Diese Maßnahmen werden in einer Bibliothek geführt, einem Vertrauensniveau zugeordnet und über den gesamten Lebenszyklus der Anwendung gepflegt.

Was die Software liefert

Inhaltlich ist erstaunlich viel vorhanden – nur nicht unter den Namen, die die Norm verwendet:

Erwartung der Norm	Stand bei Focus Family
Anforderungen und Umfeld spezifiziert	**erfüllt** – Anforderungsspezifikation mit stabilen Kennungen, Abnahmekriterien, Testnachweisen, Rückverfolgbarkeitsmatrix und einer Konkordanz, die die durchnummerierten Altverweise in Code und Dokumentation auflöst
Risiken bewertet	**erfüllt** – 28 Bedrohungsszenarien mit Wert, Akteur, Angriff, Maßnahme und **benanntem Restrisiko**
Maßnahmen mit Prüfungen verknüpft	**faktisch erfüllt** – zu jeder Sicherheitsmaßnahme existiert ein Test, der fehlschlägt, sobald sie entfernt wird
Anwendungsspezifisches Rahmenwerk (ANF)	**nicht vorhanden**
Ziel-Vertrauensniveau festgelegt	**nicht vorhanden**
Sicherheit über den Lebenszyklus	**gelebt, nicht beschrieben**
Unabhängige Prüfung	**teilweise** – mehrere dokumentierte Prüfrunden einschließlich werkzeuggestützter Zweitprüfungen, jedoch alle vom Hersteller veranlasst

Die Verknüpfung „Maßnahme ↔ Prüfung" verdient eine Hervorhebung, weil sie das ist, was die Norm im Kern verlangt, und weil sie selten sauber umgesetzt wird: Zu den 612 Testdateien gehören gezielte Angriffstests – Zugriff über fremde Kennungen, Rechteanmaßung durch manipulierte Anfragen, Wiedereinspielen abgefangener Gerätenachweise, Umgehung der Vier-Augen-Freigabe, Zugriff über fremde Server-Instanzen, Kontoänderungen oberhalb der eigenen Rechte, Anfragefälschung gegen jede Verwaltungsaktion, Rechenzeitunterschiede bei der Anmeldung, Zugriffe auf interne Adressen über Schnittstellen-Verbindungen, Freigabe einer Schnittstelle durch die Person, die sie zuletzt geändert hat, Datenabfluss über den Änderungs-Feed an der Fallsichtbarkeit vorbei. Jeder dieser Tests **belegt** eine Sicherheitsaussage, statt sie nur zu behaupten.

Was Sie selbst leisten müssen

27034 richtet sich primär an den Hersteller. Für Sie relevant: Sie sollten vom Hersteller verlangen können, dass er Ihnen das angestrebte **Vertrauensniveau** nennt und darlegt, welche Maßnahmen dafür geprüft werden. Diese Auskunft können wir derzeit nur beschreibend geben, nicht in der von der Norm vorgesehenen Struktur.

Wo es aktuell hakt

Die Anforderungsspezifikation liegt bei (`docs/requirements/REQUIREMENTS.de.md`). Sie führt funktionale, nichtfunktionale und Sicherheitsanforderungen mit stabilen Kennungen und Testnachweisen. Die Ursprungsdokumente der Paragrafenverweise („§120", „§175") sind nicht überliefert; eine Konkordanz löst diese Verweise aus ihrem Verwendungskontext auf. Sie ist eine Rekonstruktion, nicht das Original.

Es gibt keine Maßnahmenbibliothek und kein Vertrauensniveau. Die Substanz ist vorhanden, die Form fehlt. Aus dem Bedrohungsmodell und den vorhandenen Prüfungen lässt sich eine normkonforme Struktur mit überschaubarem Aufwand ableiten – hier liegt das beste Verhältnis von Aufwand zu Nutzen aller vier Normen.

ISO/IEC 25010 – Software-Produktqualität

Die Norm beschreibt Produktqualität in neun Merkmalen. Bewertung im Einzelnen:

Funktionale Eignung – erfüllt

Der fachliche Ablauf (Vorbereiten → Begleiten → Nachbereiten → Dokumentieren) ist vollständig abgebildet, mit vier Handbüchern und einem Schnittstellenhandbuch in zwei Sprachen dokumentiert und durch über 2.200 Servertests sowie 612 Testdateien insgesamt abgesichert. Das Verhältnis von C#-Testcode zu C#-Produktivcode liegt bei 0,63 (130.159 zu 207.796 Zeilen) – ein für Fachanwendungen ungewöhnlich hoher Wert.

Leistungseffizienz – teilweise

Umgesetzt sind die üblichen Vorkehrungen: über 110 Datenbankindizes, lesende Abfragen ohne Änderungsverfolgung, Streaming-Verarbeitung für große Dateien statt vollständigem Laden in den Speicher, Speicherkontingente je Organisation mit atomarer Reservierung, Kennzahlen zu Speicherplatz und Prozessgröße über

eine Überwachungsschnittstelle.

Lastnachweis: Ein Lasttest mit realistisch angemeldeten Geräten und signierten Anfragen (`docs/server/CAPACITY.de.md`) blieb bei 50 gleichzeitig synchronisierenden virtuellen Fachkräften fehlerfrei mit einer Abrufdauer unter 250 ms (p95). Daraus folgt die Dimensionierungsaussage: Bis zu 200 gleichzeitig arbeitende Fachkräfte mit dem Standard-Synchronisationsintervall sind auf einem Server mit 4 vCPUs und 8 GB RAM mit großer Reserve abgedeckt. Für größere Einrichtungen sollten Sie die Messung mit dem mitgelieferten Skript auf Ihrer Zielhardware wiederholen.

Was fehlt: Bei Überlast antwortet der Server mit Fehlern, statt Anfragen warten zu lassen, weil der Verbindungspool so groß ist wie die Verbindungsgrenze der Datenbank (Befund F-32).

Kompatibilität – erfüllt

Focus Family läuft aus einer Codebasis auf iOS, iPadOS, Android, macOS und Windows, dazu eine Apple-Watch-Begleit-App. Der Datenaustausch ist bewusst offen gehalten: Fallexporte als JSON mit mitgeliefertem Schema, Zeit- und Fahrtdaten als dokumentiertes CSV, Dokumente als PDF, DOCX und XLSX. Die Schnittstelle ist versioniert und liefert 71 strukturierte Fehlercodes.

Für die Anbindung eigener Fachverfahren liegen maschinenlesbare Schnittstellenbeschreibungen im Format OpenAPI 3.1 bei (`docs/api/openapi.v1.json` für App und Verwaltung, `docs/api/openapi.integration-v1.json` für die Integrations-API mit eigenen Fehlercodes); automatische Tests stellen sicher, dass sie der ausgelieferten Schnittstelle entsprechen. Die Interoperabilität mit Fremdsystemen stützt sich auf offene Standards statt Eigenformate: CMIS 1.1 für DMS und E-Akte, XÖV/xdomea 3.1.0 und 4.0.0 mit Prüfung gegen das amtliche Schema, SCIM 2.0, iCalendar, Syslog nach RFC 5424/5425 und CEF, CloudEvents mit Standard-Webhooks-Signatur. Jede Schnittstelle ist in eigener Dokumentation beschrieben. CMIS und SFTP sind gegen echte Testsysteme geprüft; XTA 2 und FIT-Connect bislang nur gegen Nachbildungen der Spezifikation (Befund F-33).

Interaktionsfähigkeit – teilweise

Positiv: Oberflächen von App, Desktop-Anwendung und Verwaltungsoberfläche in sieben Sprachen (Deutsch, Englisch, Spanisch, Französisch, Türkisch, Russisch, Polnisch), durchgängige Tablet- und Desktop-Layouts, Bedienhilfen und Erklärtexte an Ort und Stelle, vier zielgruppengerechte Handbücher.

Barrierefreiheit, Stand der Prüfung: Alle rein symbolischen Bedienelemente tragen Beschriftungen für Bildschirmlesegeräte (60 in der mobilen App, 30 in der Desktop-Anwendung), Formularfelder sind beschriftet, die Verwaltungsoberfläche hat Sprungmarke und sichtbaren Tastaturfokus, Schrift skaliert mit der Systemeinstellung, heller und dunkler Modus sind vorhanden. Eine Erklärung zur Barrierefreiheit liegt bei; ein automatischer Test schlägt fehl, sobald ein symbolisches Bedienelement ohne Beschriftung hinzukommt.

Was fehlt, und für Sie wichtig: Es gibt **keine Prüfung mit echten Hilfsmitteln** (VoiceOver, TalkBack, NVDA, JAWS), Kontrastwerte sind nicht gemessen, Vorlesereihenfolge und Überschriftenhierarchie der mobilen Ansichten sind nicht geprüft, erzeugte PDF-Dokumente sind nicht getaggt, und Zeichenflächen (Skizzen, Handschrift, Unterschriften) haben keine gleichwertige Alternative. Focus Family ist damit **teilweise konform** mit EN 301 549.

Wenn Sie ein öffentlicher Träger sind, betrifft Sie das unmittelbar: Die Barrierefreie- Informationstechnik-Verordnung verpflichtet Sie für Ihre eingesetzte IT, und das Barrierefreiheitsstärkungsgesetz erweitert die Anforderungen. Übernehmen Sie die genannten Einschränkungen in Ihre eigene Erklärung zur Barrierefreiheit; Einzelheiten stehen im Befund F-13 des Prüfberichts.

Zuverlässigkeit – erfüllt

Die wichtigste Eigenschaft für Ihren Einsatz: **Ein Serverausfall unterbricht die Fallarbeit nicht.** Die Apps arbeiten vollständig gegen ihren lokalen verschlüsselten Datenbestand; die Synchronisation ist Abgleich im Hintergrund, keine Voraussetzung für das Arbeiten.

Weiter abgesichert: Gleichzeitige Änderungen führen zu einem sichtbaren Konflikt statt zu stillem Überschreiben. Wiederholte Übertragungen erzeugen keine Duplikate. Löschungen hinterlassen Grabsteine, sodass ein lange offline gewesenes Gerät gelöschte Daten nicht wiederbeleben kann. Die Wiederherstellung eines App-Backups prüft die Datei **vollständig, bevor** irgendetwas überschrieben wird – ein falsches Passwort kann keinen halben Bestand zerstören. Die Bereitschaftsprüfung des Servers prüft tatsächlich die Datenbank. Die Anmeldung einer Serverinstallation beim Lizenzserver wird vor dem Einlösen des Installationsschlüssels vorgemerkt und ein abgebrochener Versuch lässt sich mit demselben Schlüssel wiederholen; ein nicht lesbarer Lizenzzustand führt zu einer Fehlermeldung statt zu einer stillen Neuanmeldung.

Einschränkung: Der Server ist als Einzelinstanz ausgelegt. Für Hochverfügbarkeit müssen Sie selbst sorgen.

Sicherheit – erfüllt

Siehe Abschnitt ISO/IEC 27001. Ergänzend zum dortigen Bild: Nachvollziehbarkeit und Nicht-Abstreitbarkeit sind über das Audit-Protokoll, Dokumentsignaturen und Prüfsummen abgedeckt – mit der im 27001-Abschnitt genannten Einschränkung zum Schreibschutz des Protokolls.

Wartbarkeit – erfüllt

17 klar geschnittene Teilprojekte mit sauberer Schichtung (plattformfreie Fachlogik, getrennte Infrastruktur, getrennte Oberflächen je Plattform). Durchgängige Korrelationskennungen machen einen Vorgang über Client, Server und Protokoll hinweg nachvollziehbar. Die Testabdeckung wird gemessen: 88,0 % der Zeilen und 68,1 % der Zweige. Ein verbindliches Regelwerk für statische Sicherheitsanalyse und ein Scan der Container-Abbilder laufen im Bauvorgang.

Flexibilität – erfüllt

Fünf Plattformen aus einer Codebasis. Selbstbetrieb ohne Herstellerabhängigkeit. Zentrale Konfigurationspunkte für Erscheinungsbild und Organisationsdaten. Organisationsweite Einstellungen lassen sich zentral vorgeben und auf den Geräten festsetzen.

Sicherheit im Sinne von Gefahrlosigkeit – teilweise

Focus Family trifft bewusst **keine fachlichen Entscheidungen**: keine Diagnosen, keine rechtlichen Bewertungen, keine Bewertung von Personen. Das steht ausdrücklich in der Produktbeschreibung und ist in der Funktionalität durchgehalten. Sicherheitsrelevante Mechanismen scheitern im Zweifel geschlossen (kein Virenscanner → kein Upload; fehlender Signaturschlüssel → Ablehnung).

Was fehlt: eine dokumentierte Gefährdungsbetrachtung für den Fachkontext. Beispiel: Welche Folge hat der Verlust einer Verlaufsdokumentation für ein laufendes Hilfeverfahren, und welche Vorkehrung adressiert das? Technisch ist vorgesorgt (keine stille Datenlöschung, Konfliktanzeige, Grabsteine), die fachliche

Herleitung ist aber nicht aufgeschrieben.

ISO/IEC 29147 und 30111 – Umgang mit Schwachstellen

Worum es geht

Die beiden Normen bilden ein Paar. **29147** regelt die Außenseite: Wie kann jemand dem Hersteller eine Sicherheitslücke melden, und wie informiert der Hersteller die Betreiber? **30111** regelt die Innenseite: Wie nimmt der Hersteller eine Meldung an, bewertet, behebt und veröffentlicht sie?

Für Sie als Betreiber ist das keine Formalie. Ihr eigenes ISMS verlangt, dass Sie über Sicherheitsupdates Ihrer eingesetzten Software informiert werden und diese bewerten können.

Stand

Anforderung	Norm	Stand
Veröffentlichte Richtlinie zur Schwachstellenmeldung	29147	**vorhanden** (`SECURITY.md` im Projekt, verlinkt von der Produktseite)
Meldeweg (Kontaktadresse, `security.txt`)	29147	**vorhanden** (`security@software-notion.de`, `/.well-known/security.txt`)
Empfangsbestätigung und Reaktionszeiten	29147	**veröffentlicht** (Bestätigung 3 Werktage, Bewertung 10 Werktage, Behebung 14/30 Tage nach Schweregrad)
Koordinierte Offenlegung	29147	**Frist von 90 Tagen veröffentlicht, noch nie angewandt**
Sicherheitsmeldungen an Betreiber	29147	**Vorlage und Zustellweg festgelegt, noch keine Meldung ausgeliefert**
Annahme und Erfassung von Meldungen	30111	**Postfach eingerichtet, Meldefunktion in Admin-Panel, App und Desktop**
Verifikation gemeldeter Schwachstellen	30111	**gelebte Praxis**
Behebung mit Wirksamkeitsnachweis	30111	**gelebte Praxis**
Bereitstellung der Behebung	30111	**Weg festgelegt (signiertes Update mit Rückstufungsschutz), noch nicht für eine Sicherheitsbehebung genu**
Beschriebener Prozess mit Rollen und Fristen	30111	**vorhanden** (`docs/security/VULNERABILITY-HANDLING.md`)
Schweregradbewertung (CVSS v3.1)	30111	**festgelegt**

Was faktisch schon funktioniert

Der inhaltliche Teil von 30111 wird gelebt und ist belegt: mehrere dokumentierte Prüfrunden, darunter eine Gesamtprüfung in sieben Teilprüfungen mit 83 Einzelbefunden, eine werkzeuggestützte Zweitprüfung am 8. Oktober 2026 und zuletzt mehrere Prüfrunden der Integrationsschnittstellen vom 28. Oktober bis 1. November 2026; jeder Befund wurde vor der Behebung am Code bestätigt, behoben und, wo möglich, mit einem Test abgesichert, der bei Rücknahme der Behebung fehlschlägt. Die wenigen bewusst offenen Restpunkte sind im Prüfbericht benannt. Dazu läuft bei jedem Bau des Produkts eine automatische Prüfung aller Fremdbibliotheken gegen bekannte Schwachstellen – ein Fund **bricht den Bauvorgang ab**, und zwar bereits ab Schweregrad „niedrig". Das ist strenger als üblich. Ergänzend prüfen eine statische Sicherheitsanalyse den eigenen Code und ein Scan die Container-Abbilder; beide brechen bei nicht begründeten Funden ab.

Was das für Sie heute bedeutet

Drei praktische Punkte, die Sie einplanen sollten:

1. **Melden können Sie sofort.** Der Meldeweg ist `security@software-notion.de`, veröffentlicht in `security.txt` und in der Meldungsrichtlinie; im Admin-Panel, in der App und auf dem Desktop gibt es dafür eine Meldefunktion, die technische Angaben ohne Fall- oder Personendaten zusammenstellt. Nehmen Sie die Adresse in Ihre Lieferantenakte auf.
2. **Sicherheitsmeldungen zu Auslieferungen sind vorbereitet, aber noch nie verschickt.** Vorlage und Zustellweg sind festgelegt; da bisher keine Auslieferung eine gemeldete Schwachstelle schließen musste, gibt es noch kein Beispiel. Vereinbaren Sie mit uns, an welche Adresse Ihres Hauses solche Meldungen gehen sollen.
3. **Die Reaktionszeiten sind veröffentlicht, aber nicht vertraglich.** Empfangsbestätigung in drei Werktagen, Bewertung in zehn Werktagen, Behebung in 14 Tagen bei kritischen und 30 Tagen bei hohen Schweregraden. Wenn Ihr ISMS Fristen bei Zulieferern verlangt, nehmen Sie diese Werte in den Vertrag auf.

Die Außenseite nach 29147 ist damit eingerichtet; was fehlt, ist der Nachweis aus dem Betrieb, weil noch kein Vorfall den Prozess durchlaufen hat. Das ist der Grund für die Einstufung „eingerichtet, noch nicht erprobt".

Wo Focus Family Ihre Zertifizierung aktuell erschwert

Dies ist die Liste, um die es Ihnen als Prüfer eigentlich geht. Sie enthält alles, was ein Auditor bei Ihnen zu einer Abweichung oder einer Auflage machen könnte.

#	Punkt	Betroffene Maßnahme	Ihr Handlungsbedarf
1	Sicherheitsmeldungen zu Versionen vorbereitet, noch nicht ausgeliefert	29147	Zustellweg mit uns vereinbaren
2	Barrierefreiheit teilweise umgesetzt, nicht mit Hilfsmitteln geprüft	25010, EN 301 549, BITV 2.0	Erklärung zur Barrierefreiheit liegt bei; verbleibende Einschränkungen in Ihre eigene Erklärung übernehmen
3	Zwei-Faktor-Authentifizierung standardmäßig deaktiviert	27001 A.8.5	Bei Inbetriebnahme aktiv setzen – Pflichtschritt
4	Serverseitig keine Ende-zu-Ende-Verschlüsselung	27001 A.8.24, DSGVO Art. 32	Betreiberzugriff organisatorisch regeln und dokumentieren
5	Keine Fernlöschung verlorener Geräte	27001 A.8.1	Eigene Gerätesperre/MDM vorsehen
6	Kapazität bis 200 gleichzeitig aktive Fachkräfte belegt; bei Überlast Fehler statt Wartezeit	25010 Leistungseffizienz	Darüber eigenen Lasttest auf der Zielhardware einplanen
7	Keine Alarmierungsregeln mitgeliefert	27001 A.8.16	Eigene Schwellwerte definieren (Datenquellen sind vorhanden)
8	Server als Einzelinstanz ausgelegt	25010 Zuverlässigkeit	Wiederanlaufziele selbst festlegen
9	Kein unabhängiges externes Sicherheitsaudit	27001 A.5.35	Ggf. eigenen Penetrationstest beauftragen
10	Serverinformation ohne Anmeldung abrufbar	27001 A.8.9	Server nicht unnötig öffentlich erreichbar machen, Admin-Panel auf Intranet oder VPN beschränken
11	Bildschirmfotos nur unter Android technisch verhindert; unter iOS wird nur die Vorschau im App-Umschalter verdeckt, die Desktop-App bietet keinen Bildschirmschutz	27001 A.8.12, A.8.1	Bildschirmfotos auf verwalteten iOS-Geräten per MDM unterbinden, Regel in die Dienstanweisung aufnehmen
12	Aktenabgabe über XTA 2 und FIT-Connect nur gegen Spezifikations-Mocks geprüft	25010 Kompatibilität, 27001 A.8.29	Vor produktiver Nutzung eine Testübertragung mit der eigenen Gegenstelle durchführen

Bewusste Grenzen des Produkts

Diese Eigenschaften sind keine Versäumnisse, sondern Entscheidungen. Sie sollten sie kennen und in Ihrer Risikobewertung abbilden.

Keine Ende-zu-Ende-Verschlüsselung. Wer administrativen Zugriff auf Serverprozess, Datenbank, Dateisystem oder Schlüsselmaterial hat, kann synchronisierte Inhalte lesen. Die Kennzeichnung eines Eintrags als „privat" schützt vor **anderen Anwendenden** – einschließlich Leitung und aller Administrationsrollen –, nicht vor dem Betreiber Ihrer Infrastruktur. Die Software stellt das an keiner Stelle anders dar.

Keine Fernlöschung. Der Entzug eines Gerätezugangs wirkt auf dem Server sofort, auf einem dauerhaft offline gehaltenen Gerät jedoch erst bei der nächsten Verbindung. Bis dahin schützen lokale Verschlüsselung, App-Sperre und die begrenzte Gültigkeit der Offline-Berechtigung. Wir versprechen ausdrücklich **keine** sofortige Fernlöschung.

Serverinhalte sind auf Anwendungsebene nicht verschlüsselt. Der Schutz ruhender Daten auf dem Server erfolgt über die Verschlüsselung Ihres Datenträgers – Dateianhänge ausgenommen, die zusätzlich anwendungsseitig verschlüsselt sind. Die Verschlüsselung des Datenbank-Volumes liegt in Ihrer Verantwortung.

Kein Zwang, online zu sein. Das ist eine Stärke, hat aber eine Kehrseite: Daten auf einem Gerät, das nie synchronisiert, existieren nur dort. Weil die App-Daten weder in Cloud- noch in Computer-Backups noch in eine Geräteübertragung gelangen, startet ein neues Gerät mit der Einrichtung; Daten kommen per App-Backup oder Synchronisation zurück. Ihre Vorgaben zur Synchronisationshäufigkeit und zu App-Backups sind deshalb auch eine Datensicherungsmaßnahme.

Keine Löschung in Zielsystemen. Was eine Schnittstelle an ein DMS, eine E-Akte, ein Jugendamt oder ein anderes Fremdsystem übermittelt hat, löscht Focus Family dort nicht. Die endgültige Löschung eines Falls entfernt die Kopien innerhalb von Focus Family; für die Zielsysteme nennt das Zustellverzeichnis die Empfänger, und auf Wunsch meldet ein Webhook-Ereignis ohne Inhalt die beantragte Löschung. Aufbewahrung und Löschung in den Zielsystemen verantworten Sie.

Keine Analyse-, Tracking- oder Werbebestandteile. Es gibt keine Telemetrie an den Hersteller. Absturzberichte gehen ausschließlich an **Ihren** Server, enthalten nur technische Felder und werden bereits auf dem Gerät bereinigt – keine Falldaten, keine Namen, keine Inhalte. Die Übermittlung ist standardmäßig aktiv und in den Einstellungen jeder Anwendung abschaltbar.

Datenschutz und Offenheit

Ein eigener Abschnitt, weil beides ausdrücklich Produktziel ist.

Keine Herstellerbindung Ihrer Daten

- **Selbstbetrieb.** Der Server läuft in Ihrer Infrastruktur. Es gibt keine Hersteller-Cloud, an die Falldaten fließen, und keinen Weg, über den wir auf Ihre Inhalte zugreifen könnten.
- **Offene Exportformate.** Fallexporte als JSON mit **mitgeliefertem Schema**; Zeit- und Fahrtdaten als CSV mit dokumentierter Spaltenbelegung; Dokumente als PDF, DOCX und XLSX. Sie können Ihren Bestand jederzeit vollständig herausziehen und in einem anderen System weiterverwenden.
- **Dokumentiertes Synchronisationsprotokoll.** Rund 470 Zeilen Protokollbeschreibung, dazu ein eigenes Vertragsmodul mit 71 benannten Fehlercodes und eine Schnittstellenbeschreibung im Format OpenAPI 3.1.
- **Standardschnittstellen.** REST/JSON mit OpenAPI-Beschreibung, CMIS 1.1, XÖV/xdomea, SCIM 2.0, iCalendar und Syslog/CEF, jeweils mit eigener Dokumentation und Konfigurationsexport ohne Geheimnisse.
- **Dokumentiertes Datenbankschema und dokumentierter Migrationsweg.** Ein Datenbankauszug ist ohne unsere Mitwirkung auswertbar.

Datenschutz als Funktionsbestandteil

Der vollständige Ablauf für Betroffenenrechte nach Art. 15–21 DSGVO ist im Produkt umgesetzt, nicht nur beschrieben: Suche, Identitätsprüfung, Zusammenstellung, Prüfung auf Nennung Dritter nach Art. 15 Abs. 4, Schwärzung, Freigabe im Vier-Augen-Prinzip, verschlüsselte Übergabe mit Einmal-Download, automatische Löschung nach Fristablauf, lückenloses Protokoll jedes Zugriffs. Eine Auskunft kann mehrere betroffene Personen umfassen, was dem familienbezogenen Zuschnitt Ihrer Fälle entspricht. Ist die Verarbeitung eines Datensatzes nach Art. 18 eingeschränkt, sperrt der Server auch Abruf und Existenzprüfung seiner Anhänge über die Geräteschnittstelle; die Antwort gleicht der für eine unbekannte Datei. Das Auskunftspaket nennt aus dem Offenlegungsverzeichnis die Empfänger, an die Schnittstellen Daten der betroffenen Personen übermittelt haben, mit Zweck und Rechtsgrundlage zum Zeitpunkt der Übermittlung.

Wo Offenheit heute endet

Ehrlichkeitshalber: Der Quellcode ist **nicht** offengelegt. Eine maschinenlesbare Stückliste der Fremdbibliotheken im Format CycloneDX wird im Bauvorgang erzeugt und auf Anfrage bereitgestellt; die Übersicht der verwendeten Fremdbibliotheken wird automatisch gegen die tatsächlich verwendeten Versionen geprüft.

Offene Punkte und geplante Verbesserungen

Der Vollständigkeit halber, mit ehrlicher Einordnung des Aufwands. Eine Terminzusage ist damit nicht verbunden; fragen Sie uns nach dem aktuellen Stand.

Vorhaben	Wirkung	Aufwand
Zwei-Faktor-Authentifizierung als Voreinstellung	Sichere Grundeinstellung	gering
Verbindungspool mit Gegendruck, weniger Protokollvolumen in Produktion	Wartezeit statt Fehler bei Überlast	gering
Reduzierte Serverinformation vor der Anmeldung	Erschwert die Erkundung	gering
Abnahme von XTA 2 und FIT-Connect gegen echte Gegenstellen	Belegt die Aktenabgabe im Verwaltungsverbund	mittel
Alarmregeln mitliefern, Anwendungsprotokolle weiterleiten	Überwachung ohne eigene Regelarbeit	mittel
Maßnahmenbibliothek und Vertrauensniveau ableiten	Macht 27034 argumentierbar	mittel
Barrierefreiheit mit Hilfsmitteln prüfen, Kontraste messen, PDF taggen	Schließt die verbleibende BITV-Lücke	hoch
Unabhängiger Penetrationstest	Externe Bestätigung	hoch

Nachweisverzeichnis

Zu jeder Aussage dieses Dokuments das Artefakt, mit dem sie belegt ist. Alle genannten Unterlagen liegen dem Produkt bei oder werden auf Anfrage bereitgestellt.

Aussage	Nachweis
Verschlüsselungsverfahren und Schlüsselverwaltung	Sicherheitsdokumentation, Abschnitte Verschlüsselungsmodell und Schlüsselverwaltung
Bedrohungen und Restrisiken	Bedrohungsmodell des Servers, 28 Szenarien, davon sieben zu den Schnittstellen
Zugriffs- und Rechtemodell	Berechtigungsdokumentation und Autorisierungsdokumentation
Synchronisation und Konfliktbehandlung	Protokolldokumentation der Synchronisation
Wirksamkeit der Sicherheitsmaßnahmen	Automatisierte Testreihe, 612 Testdateien, davon gezielte Angriffstests
Testabdeckung, statische Analyse, Abbild-Scan	Übersicht der Qualitäts- und Sicherheitsprüfungen (`docs/security/QUALITY-GATES.de.md`) mit Berichten je Lauf
Last und Kapazität	Messbericht mit Dimensionierungsaussage (`docs/server/CAPACITY.de.md`)
Schnittstellenbeschreibung	`docs/api/openapi.v1.json` und `docs/api/openapi.integration-v1.json` (OpenAPI 3.1)
Schnittstellen zu Fremdsystemen	Schnittstellendokumentation je Schnittstelle (`docs/integration/`), Schnittstellenhandbuch, Datenschutz und Sicherheit der Schnittstellen mit Vorlagen für DSFA und Verarbeitungsverzeichnis sowie Härtungs-Checkliste (`docs/integration/SECURITY-PRIVACY.de.md`), Entscheidung D16
Interne Sicherheitsprüfungen	Auditberichte mit Einzelnachweis je Befund, Gesamtprüfung vom 3. Oktober 2026; werkzeuggestützte Zweitprüfung vom 8. Oktober 2026 sowie Prüfungen der Desktop-Aktualisierung, der Paddle-Abrechnung und der Löschaufträge vom 22. bis 24. Oktober 2026 und Prüfrunden der Integrationsschnittstellen vom 28. Oktober bis 1. November 2026, jeweils mit Behebungen und Regressionstests im Änderungsprotokoll
Anmeldung über den Identitätsanbieter	Technisches Handbuch, Kapitel Single Sign-On; Berechtigungsdokumentation
Technische und organisatorische Maßnahmen (Art. 32)	Im Admin-Panel aus Ihrer Live-Konfiguration erzeugbar
Auftragsverarbeitung	AVV-Vorlage, im Admin-Panel erzeugbar
Löschkonzept	Im Admin-Panel aus Ihrer Konfiguration erzeugbar
Betroffenenrechte	Dokumentation des Auskunftsverfahrens
Datensicherung und Wiederherstellung	Verfahrensdokumentation mit durchgeführtem Wiederherstellungstest
Schwachstellenmeldung und -behandlung	Meldungsrichtlinie (`SECURITY.md`), `/.well-known/security.txt`, Behandlungsprozess (`docs/security/VULNERABILITY-HANDLING.md`), Vorlage für Sicherheitsmeldungen
Barrierefreiheit	Erklärung zur Barrierefreiheit (`docs/ACCESSIBILITY.md`), automatischer Test auf fehlende Beschriftungen (`AccessibilityLabelTests`)
Notfallabläufe	Sechs Ablaufbeschreibungen für die wahrscheinlichsten Vorfälle
Inbetriebnahme und Betrieb	Technisches Handbuch und Betriebsablaufplan
Fremdbibliotheken und Lizenzen	Übersicht der Drittanbieterkomponenten (automatisch gegen die verwendeten Versionen geprüft), Stückliste im Format CycloneDX
Anforderungen und Nachverfolgbarkeit	Anforderungsspezifikation (`docs/requirements/REQUIREMENTS.de.md`) mit Rückverfolgbarkeitsmatrix und Konkordanz der Altverweise
Zeitsynchronisation	Technisches Handbuch, Voraussetzungen und Abschnitt „Zeitsynchronisation prüfen“; Anforderung NFR-OPS-01
Diese Bewertung im Detail	Begleitdokument „Befunde und Maßnahmenplan"

Fragen, die Sie uns stellen sollten

Wenn Sie diese Prüfung ernsthaft führen, sind das die Punkte, an denen Sie nachhaken sollten. Wir haben sie bewusst selbst aufgeschrieben.

1. Wie weisen Sie den Schreibschutz des Audit-Protokolls nach?
2. Über welchen Weg und in welcher Frist melden wir Ihnen eine Sicherheitslücke?
3. Wie erfahren wir, dass eine neue Version eine Sicherheitslücke schließt?
4. Welche Reaktionszeiten sagen Sie nach Schweregrad zu, und stehen sie im Vertrag?
5. Können Sie uns eine maschinenlesbare Stückliste aller Fremdbibliotheken liefern?
6. Wie ist der Stand zur Barrierefreiheit, und gibt es eine belastbare Planung?
7. Liegt ein unabhängiger Sicherheitstest vor, und dürfen wir den Bericht sehen?
8. Wie sind die Anforderungen mit Umsetzung und Tests verknüpft, und wie lösen Sie die Paragrafenverweise in Code und Dokumentation auf?
9. Für welche Größenordnung ist das System belegt getestet?
10. Wie stellen Sie sicher, dass die Angaben in diesem Dokument aktuell bleiben?
11. Wie bleibt die Verwaltung erreichbar, wenn unser Identitätsanbieter ausfällt, und wer darf dann noch zugreifen?
12. Welche Daten verlassen über Schnittstellen unsere Installation, wer gibt das frei, und wie erfahren betroffene Personen davon?

Kontakt und Gültigkeit

Dieses Dokument beschreibt den Produktstand 1.3.0 (Build 26302), Prüfstand 1. November 2026. Es verliert seine Aussagekraft mit jeder wesentlichen Produktänderung. Bitte fordern Sie vor einer Vergabeentscheidung eine aktuelle Fassung an.

Software Notion · Sebastian Kruse · Kornblumenring 40 · 31600 Uchte · Deutschland · https://software-notion.de

Eine englische Fassung dieses Dokuments stellen wir auf Anfrage bereit.